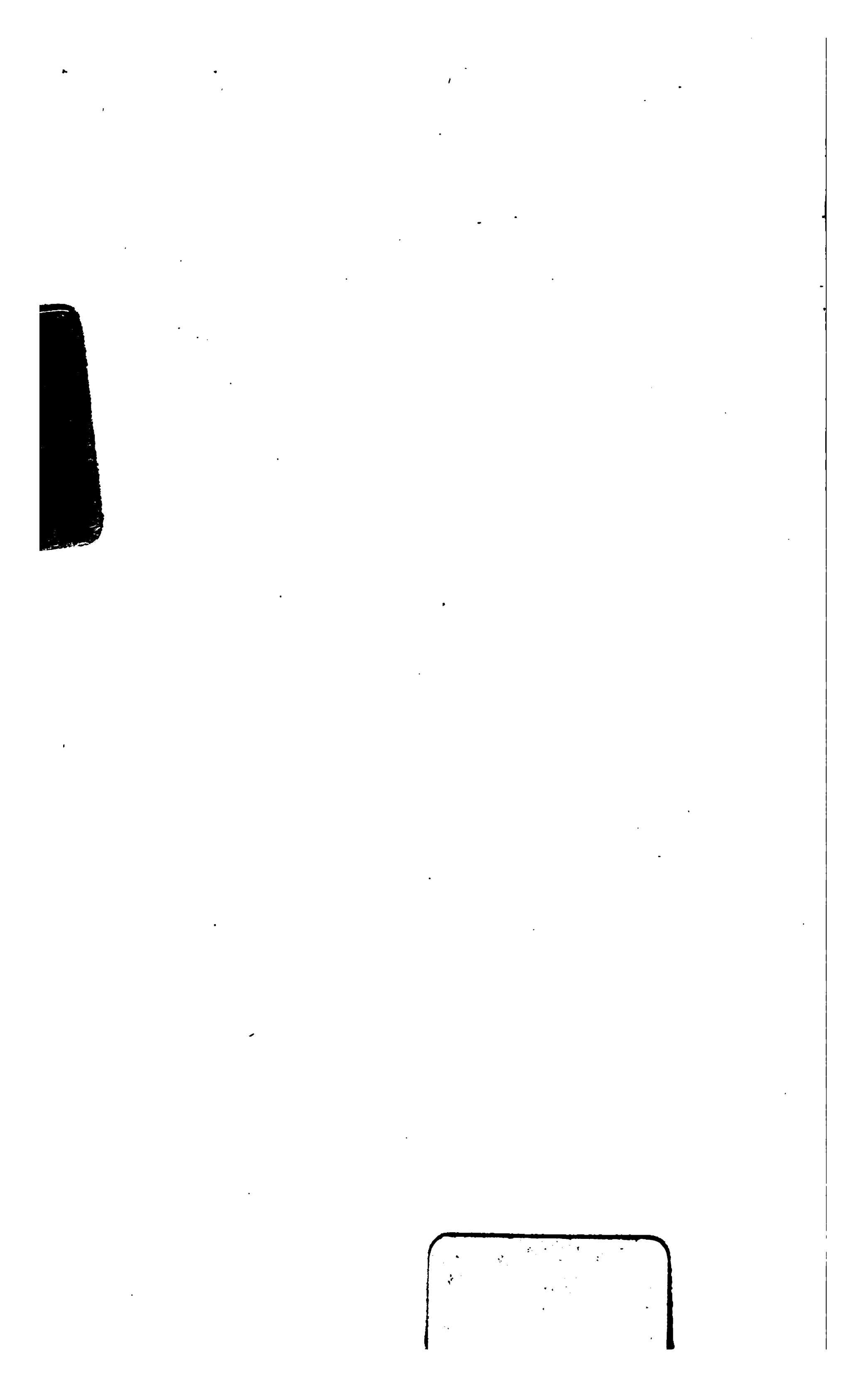


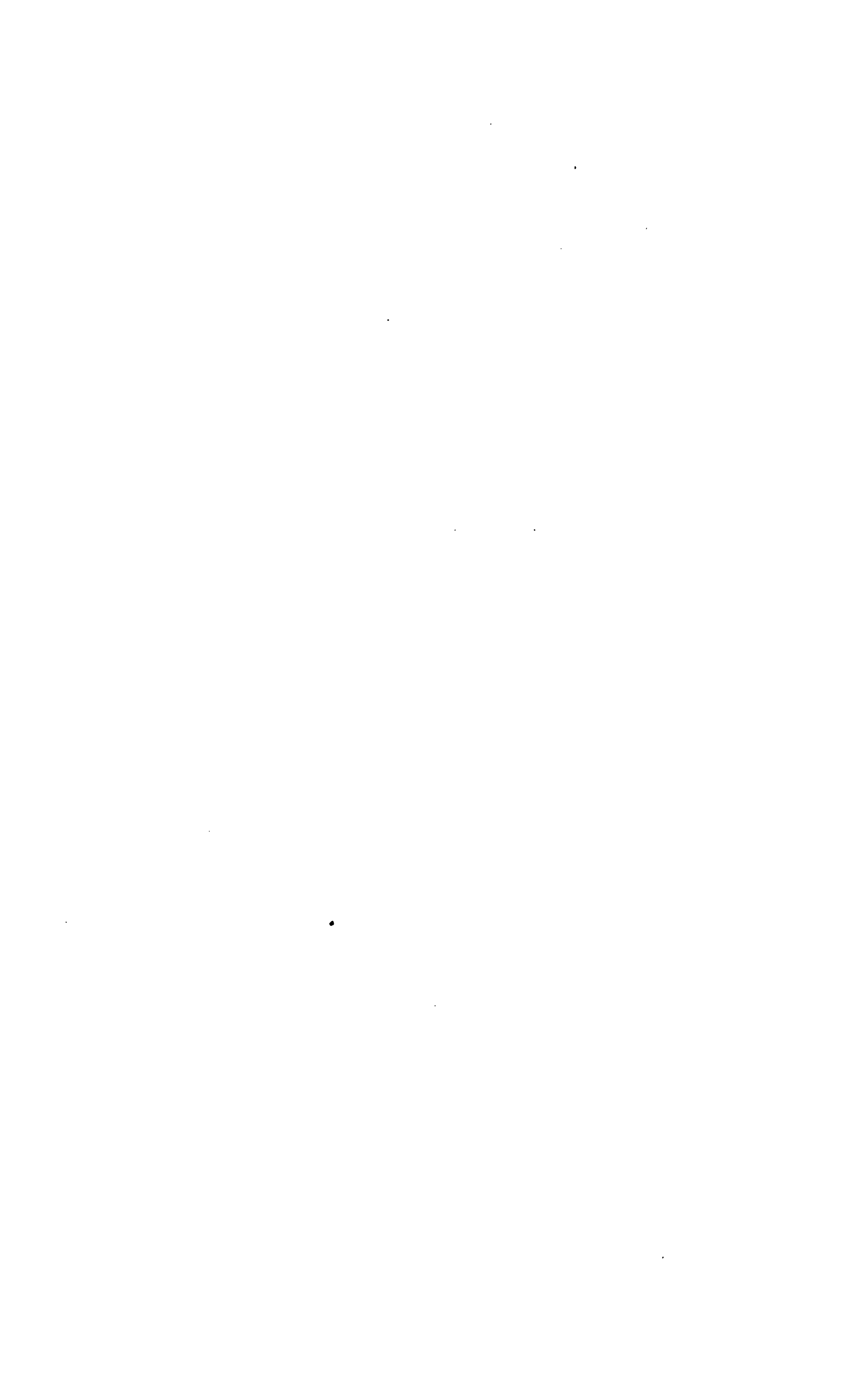
OFO

Bachmann









DIE LEHRE

VON DER

KREISTHEILUNG

UND IHRE BEZIEHUNGEN

ZUR

ZAHLENTHEORIE.

ACADEMISCHE VORLESUNGEN

VON

Dr. PAUL BACHMANN,

A. O. PROFESSOR AN DER UNIVERSITÄT BRESLAU.



LEIPZIG,

DRUCK UND VERLAG VON B. G. TEUBNER.

1872.

VORREDE.

Die Lehre von der Kreistheilung, obwohl eins der interessantesten Gebiete, welche in neuerer Zeit der Mathematik hinzugefügt worden sind, weil Geometrie, Arithmetik und Algebra in wunderbarer Weise darin in Wechselbeziehung stehen, ist doch bisher nur wenig in weiteren Kreisen bekannt und beachtet worden. Wenn hiervon der Grund einerseits darin zu suchen ist, dass andere, gleichzeitig entstandene, Disciplinen von grosser Wichtigkeit einen bedeutenden Theil des Interesses absorbirt haben, sowie darin, dass alle der Zahlentheorie angehörenden Gebiete ihrer grossen Abstractheit wegen eine verhältnissmässig nur geringe Anziehungskraft auszuüben pflegen, so ist ohne Zweifel von nicht geringerem Gewichte der Umstand, dass bisher die betreffenden Untersuchungen, welche sehr zahlreich sind, noch nicht gesammelt und in passender Verbindung, sondern nur in einzelnen Abhandlungen, in den verschiedenen mathematischen Zeitschriften zerstreut, dem Publicum dargeboten worden sind. Diese Erwägung und der Wunsch, eine Disciplin, welche dem Verfasser selbst grosses Interesse einflösst, auch Anderen näher zu bringen, haben ihn bewogen, die hier folgenden Vorlesungen über Kreistheilung und höhere Arithmetik, wie sie zum Theil an hiesiger Universität von ihm gehalten worden sind, dem Druck zu übergeben. Dem Zwecke entsprechend ist dabei weniger darauf gesehen worden, Alles, was in dem Gebiete bisher gearbeitet worden, zusammenzustellen, als vielmehr, wie es bei academischen Vorlesungen angezeigt ist, auf eine passende Auswahl, durch welche jede, wesentlich in Frage kommende Seite des Gegenstandes beleuchtet, der Leser in denselben eingeführt und in den Stand gesetzt wird, sich in der vorhandenen Literatur zurecht zu finden und selbständig weiter zu arbeiten. Um jedoch

den Mangel der Vollständigkeit einigermassen auszugleichen, sind in häufigen Citaten die hauptsächlichsten Arbeiten über die behandelte Disciplin angegeben worden.

Jacobi hat über denselben Gegenstand Vorlesungen gehalten, von welchen verschiedene Hefte noch vorhanden sind. Durch die Güte des Herrn Professor Kronecker ist dem Verfasser die Durchsicht eines solchen gestattet worden, als Auswahl und Anordnung des Stoffes ihm schon ziemlich feststanden. Er hat sich dabei überzeugt, dass die wichtigsten Resultate, zu welchen Jacobi gelangt ist, gleichzeitig durch Cauchy gefunden oder seitdem durch die Arbeiten anderer Mathematiker reproducirt worden sind. Wenn gleichwohl die Publication von Jacobi's Vorlesungen wegen einer Reihe von speciellen und feinen Untersuchungen, welche ihm durchaus eigen sind, ein besonderes Interesse darbieten würde, schien es doch dem Verfasser für das Publicum wünschenswerther, auch von den Arbeiten späterer Mathematiker, namentlich von der Vervollkommnung, welche Kummer den Resultaten Jacobi's gegeben hat, unterrichtet zu werden, die Einfügung dieser Arbeiten in die Jacobi'schen Vorlesungen jedoch kaum möglich, ohne deren Character völlig zu verändern. Um indessen einer eventuellen Veröffentlichung jener Vorlesungen nicht vorzugreifen, hat er sich nur an einer Stelle (in Nr. 2 der 13. Vorlesung) erlaubt, einen Passus aus denselben herüberzunehmen, alles Uebrige ist nach andern, überall, wo es wünschenswerth schien, angegebenen Quellen gearbeitet worden.

Noch muss ein Wort über die Vorkenntnisse, welche in diesem Buche von dem Leser werden gefordert werden, hier Platz finden. Dem Verfasser sind in dieser Hinsicht folgende Gesichtspunkte massgebend gewesen. Da es ihm darauf ankommt, den Inhalt des Buches weiteren Kreisen, namentlich den Studirenden zugänglich zu machen, hat er eine verhältnissmässig geringe mathematische Bildung, aus der Algebra nur die Bekanntschaft mit den allgemeinen Sätzen über die Gleichungen, ihre Wurzeln und die symmetrischen Functionen derselben, aus der Zahlentheorie etwa mit denjenigen, auf Theilbarkeit der Zahlen und Congruenzen bezüglichen, einfachen Sätzen vorausgesetzt, welche in Dirichlet's Vorlesungen über Zahlentheorie, herausgegeben von Dedekind, die ersten 20 bis 25 Paragraphen erfüllen. Hiezu bestimmte den Verfasser zudem die Absicht, die eigenthüm-

liche Wechselbeziehung, welche zwischen der Lehre von der Kreistheilung einerseits und der höheren Arithmetik andererseits besteht, in das hellste Licht zu setzen, indem er nichts aus der letztern voraussetzen mochte, was durch die erstere ohne Zwang konnte abgeleitet werden. Alle andern arithmetischen Betrachtungen aber, welche die nothwendige Basis für die Anwendungen der Kreistheilung bilden, sind in dem Buche selbst an den betreffenden Stellen auseinandergesetzt worden.

Möge die vorliegende Arbeit dem Zwecke dienen, zu welchem der Verfasser sie bestimmt hat: Interesse für die feinen Untersuchungen über Kreistheilung zu erwecken, welche das erste Beispiel jenes wunderbaren Zusammenhanges geboten haben, der die Zahlentheorie mit den verschiedensten Gebieten der mathematischen Speculation verbindet! —

Breslau im Frühling 1872.

Inhalts-Verzeichniss.

Erste Vorlesung.

Das Problem der Kreistheilung.

Zweite Vorlesung.

Dritte Vorlesung.

Von den Einheitswurzeln und ihren einfachsten Eigenschaften.

Vierte Vorlesung.

Hilfssätze über Congruenzen. Die primitiven Wurzeln (mod. p).

Fünfte Vorlesung.

Von der Irreductibilität der Kreistheilungsgleichung.

Sechste Vorlesung.

Die Gauss'sche Methode zur Auflösung der Kreistheilungsgleichung. Die Perioden und ihre Eigenschaften.

Seite

Zehnte Vorlesung.

Anwendung der Kreistheilung zur Zerlegung der Zahlen in Quadrate.

Elfte Vorlesung.

Fortsetzung: Die Fälle $p = 6n + 1$, $p = 8n + 1$.

Zwölfte Vorlesung.

Die complexen ganzen Zahlen von der Form $a + bi$.

Dreizehnte Vorlesung.

Das Reciprocitätsgesetz der biquadratischen Reste.

Seite

Vierzehnte Vorlesung.

Die complexen Zahlen $a + b\varrho$. Das Reciprocitätsgesetz für die cubischen Reste.

Fünfzehnte Vorlesung.

Die Bildung der Periodengleichungen. Zerfällung von X in Factoren. Die Ergänzungssätze.

Sechszehnte Vorlesung.

Fortsetzung: Der Fall $p = 4n + 1$.

Sie[illegible]

Die P[illegible]

[illegible]

Die Theorie der aus [illegible]

Seite

Neunzehnte Vorlesung.

Anwendung der Theorie der complexen Zahlen auf die Kreistheilung.

Zwanzigste Vorlesung.

Zwei Anwendungen auf die Theorie der quadratischen Formen.

Erste Vorlesung.

Das Problem der Kreistheilung.

1. Die Lehre von der Kreistheilung hat die Aufgabe: die ganze Peripherie des Kreises in eine gegebene Anzahl gleicher Theile zu zerlegen., zu ihrem Gegenstande. Dafür kann man auch die Aufgabe substituiren: den ganzen Winkelraum um den Mittelpunkt, welcher vier Rechte oder 360^0 beträgt, in dieselbe Anzahl gleicher Theile zu theilen. Verbindet man die successiven Theilpunkte der Peripherie durch gerade Linien, so entsteht ein, dem Kreise eingeschriebenes, regelmässiges Vieleck von ebensoviel Seiten, als die Anzahl der gleichen Theile beträgt. Man kann also die Aufgabe der Kreistheilung auch so aussprechen: In den Kreis ein regelmässiges Vieleck von gegebener Seitenzahl einzutragen.

Diese Aufgabe ist eine der ältesten in der ganzen Mathematik, aber ihre Lösung ist nur in den einfachsten Fällen des Problems bereits den Alten (zu Euclid's Zeiten*)) bekannt gewesen. Wir wollen hier zunächst diese einfachsten Fälle zusammenstellen.

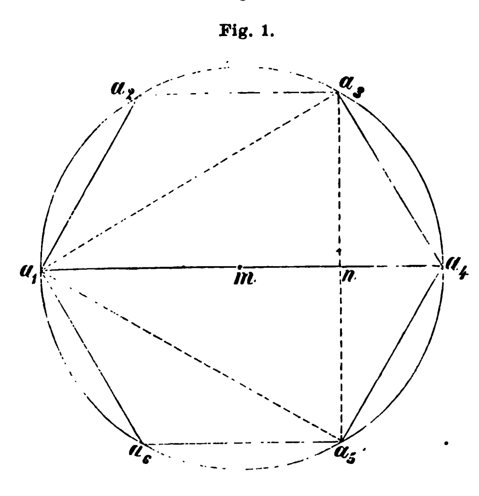
1) Man theilt den Kreis in zwei gleiche Theile durch irgend einen Durchmesser desselben, und durch zwei auf einander senkrechte Durchmesser in vier.

2) Um ihn in sechs gleiche Theile zu zerlegen oder ein reguläres Sechseck einzuschreiben, beachte man, dass jedes der congruenten Dreiecke, aus denen das letztere besteht, ein gleichschenkliges ist, mit der Sechseckseite als Basis. Da nun der Winkel an der Spitze 60^0 beträgt, muss jedes dieser Dreiecke

*) S. Euclid's Elemente, Buch IV. — In Bretschneider's Buch „die Geometrie und die Geometer vor Euclides“ §. 69 wird die Bekanntschaft mit den regelmässigen Vielecken, namentlich dem Fünfecke, schon Pythagoras zugeschrieben.

sogar ein gleichseitiges sein. Folglich ist die Sechseckseite dem Radius des Kreises gleich.

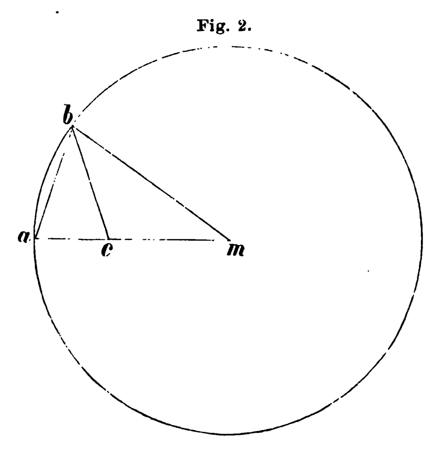
Fig. 1.



3) Denkt man sich das reguläre Sechseck $a_1\,a_2\,a_3\,a_4\,a_5\,a_6$ (Fig. 1) in den Kreis eingeschrieben und verbindet dann a_1 mit a_3, a_3 mit a_5, a_5 mit a_1, so entsteht das reguläre Dreieck. Wie leicht zu sehen, steht $a_3 a_5$ auf dem Radius $m a_4$ senkrecht und halbirt denselben in n. Man erhält folglich die Dreiecksseite, indem man durch den Mittelpunkt eines Radius die auf ihm senkrechte Sehne zieht.

4) Ist amb (Fig. 2) eins der congruenten Dreiecke, aus welchen das reguläre Zehneck besteht, so ist $\sphericalangle\, amb = 36^0$, $\sphericalangle\, mab = \sphericalangle\, mba = 72^0$. Halbirt man daher den $\sphericalangle\, mba$ durch die Linie bc, so wird $\triangle\, mcb$ gleichschenklig, ebenso wie $\triangle\, abc$. Daraus folgt $ab = bc = cm$; und aus der Aehnlichkeit der beiden Dreiecke amb und abc ergiebt sich:

Fig. 2.



$$ac : ab = ab : am$$

oder mit Rücksicht auf die gefundene Gleichheit:

$$ac : cm = cm : am.$$

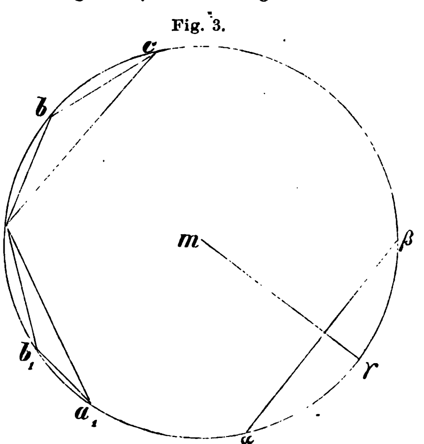
Theilt man also einen Radius am durch den sogenannten goldenen Schnitt in c nach stetiger Proportion, und schlägt um c mit dem grösseren Stücke cm einen Kreis, welcher den gegebenen in b schneide, so ist die Sehne ab die Seite des regelmässigen Zehnecks.

5) Die Summe zweier Zehntheile der Peripherie, ab und bc (Fig. 3) giebt einen Fünftheil ac, und folglich ist die Sehne ac die Seite des regelmässigen Fünfecks.

6) Ist aa_1 ein Sechstheil der Peripherie, ab_1 ein Zehntheil, so wird nach der Gleichung $\frac{1}{6} - \frac{1}{10} = \frac{1}{15}$ das Stück a_1b_1 ein Fünfzehntheil sein.

7) Man theilt irgend einen Bogen $\alpha\beta$ in zwei gleiche Theile, indem man auf die Sehne $\alpha\beta$ vom Mittelpunkte ein Loth fällt und es bis γ in der Peripherie verlängert. Diese Bemerkung lehrt, dass, wenn man die Kreisperipherie in irgend eine Anzahl n gleicher Theile getheilt hat, man jeden derselben in zwei, vier, acht, ... gleiche Theile zerlegen kann; mit andern Worten: wenn man den Kreis in n gleiche Theile zu theilen weiss, so versteht man es auch für $2n$, $4n$, $8n$, ... allgemein für $2^x \cdot n$ gleiche Theile. Wir können demnach das Problem der Kreistheilung bereits als gelöst ansehen für jede Anzahl gleicher Theile, welche in einer der Formeln

Fig. 3.



$$2^x,\ 3 \cdot 2^x,\ 5 \cdot 2^x,\ 15 \cdot 2^x$$

enthalten ist, worin 2^x jede ganze Potenz von Zwei bedeutet.

2. Diese aus der elementaren Geometrie jetzt allgemein bekannten Betrachtungen erschöpfen alle Fälle, in welchen die Lösung der Aufgabe schon Euclid bekannt war. Es ist nun höchst merkwürdig, dass es erst nach zwei Jahrtausenden Gauss gelang, weiter darüber hinauszuschreiten, und die Art, wie es geschah, ist sehr geeignet, auf den Entwicklungsgang der mathematischen Wissenschaften ein helles Licht zu werfen. Bisweilen bleibt lange Zeit, trotz anhaltender Bemühungen, ein Problem ungelöst oder eine Frage unbeantwortet, welche in irgend einem Gebiete gestellt sind. Inzwischen schreitet die Wissenschaft in anderen Richtungen unaufhaltsam fort, neue Disciplinen entstehen

und werden ausgebildet, welche ohne Zusammenhang scheinen mit jenem Probleme, bis plötzlich der Horizont sich erweitert, ein überraschender Zusammenhang zwischen scheinbar heterogenen Dingen erkannt wird und so die Frage in einem ganz anderen Gebiete, als in welchem sie ursprünglich aufgeworfen war, ihre Beantwortung findet. So ist es der Aufgabe der Kreistheilung auch ergangen. Ursprünglich eine Frage der reinen Geometrie, ist sie durch Gauss zu einer algebraischen geworden und in den innigsten Zusammenhang mit den Eigenschaften der ganzen Zahlen getreten. Dadurch wird es erklärlich, dass Gauss' betreffende Untersuchung einen Abschnitt*) seines berühmten, im Jahre 1801 erschienenen Werkes „Disquisitiones arithmeticae" bildet, welches, wie der Titel besagt, rein arithmetischen Untersuchungen gewidmet ist. Um diesen Zusammenhang verständlich machen zu können, ist es zunächst nothwendig zu zeigen, wie die geometrische Aufgabe der Kreistheilung in eine algebraische verwandelt werden kann.

Angenommen, die Kreisperipherie sei durch die Punkte $a_1, a_2, a_3, \ldots a_n$ in n gleiche Theile getheilt, eine Anzahl, welche wir nach dem zuvor über die Zweitheilung eines Winkels Gesagten jetzt und in allem Folgenden als ungerade voraussetzen können, so ist leicht zu sehen, dass, wenn man a_1 mit a_3 verbindet und diese Linie wiederholt in den Kreis einträgt, man allmählich zu allen Theilpunkten gelangen wird; denn zunächst trifft man auf die Punkte $a_5, a_7, \ldots a_n$ mit ungeradem, sodann auf die Punkte $a_2, a_4, \ldots a_{n-1}$ mit geradem Index, bis man endlich zum Punkte a_1 zurückkehrt. Kann man daher die Länge $a_1 a_3$ finden, so hat man damit die Theilung des Kreises in n gleiche Theile geleistet. Wenn wir uns nun der trigonometrischen Functionszeichen bedienen, so ist $a_1 a_3$ nichts Anderes als $2R . \sin\frac{2\pi}{n}$, wenn R den Radius des Kreises und, wie gewöhnlich, 2π die ganze Peripherie eines Kreises mit dem Radius Eins bezeichnet. Unsere geometrische Aufgabe ist hierdurch darauf reducirt, den Werth von $\sin\frac{2\pi}{n}$ zu ermitteln, wofür man auch irgend eine andere trigonometrische Function

*) Gauss disquisitiones arithmeticae, sectio VII, in seinen mathem. Werken Bd. I. pag. 412.

desselben Bogens, z. B. $\cos\frac{2\pi}{n}$, $\operatorname{tg}\frac{2\pi}{n}$ suchen kann, da man aus den Werthen dieser Grössen jenen Werth mittels der bekannten Formeln:

$$\sin\frac{2\pi}{n} = \sqrt{1-\cos^2\frac{2\pi}{n}}, \quad \sin\frac{2\pi}{n} = \frac{\operatorname{tg}\frac{2\pi}{n}}{\sqrt{1+\operatorname{tg}^2\frac{2\pi}{n}}}$$

erhält.

3. Als besonders einfach aber empfiehlt es sich, nicht die trigonometrischen Functionen $\sin\frac{2\pi}{n}$, $\cos\frac{2\pi}{n}$ selber, sondern die folgende Combination derselben: $\cos\frac{2\pi}{n} + i \cdot \sin\frac{2\pi}{n}$, in welcher $i = \sqrt{-1}$ ist, zu suchen. Findet man den Werth dieses Ausdruckes gleich $a + bi$, so hat man unmittelbar auch $\cos\frac{2\pi}{n} = a$, $\sin\frac{2\pi}{n} = b$, also die Kreistheilungsaufgabe gelöst. Für irgend einen Bogen α aber ist nach der Moivre'schen Formel

$$(\cos\alpha + i\sin\alpha)^n = \cos n\alpha + i\sin n\alpha,$$

aus welcher sich für $\alpha = \frac{2\pi}{n}$

$$\left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)^n = 1$$

ergiebt. Der gesuchte Ausdruck $\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ ist daher eine Wurzel der Gleichung:

$$x^n = 1. \tag{1}$$

Auf solche Weise wird die Kreistheilungsaufgabe durch die algebraische Aufgabe ersetzt: diese einfachste Gleichung n^{ten} Grades aufzulösen d. i. ihre Wurzeln zu bestimmen.

Es ist leicht, sämmtliche Wurzeln der Gleichung (1) durch trigonometrische Functionen der Vielfachen von $\frac{2\pi}{n}$ auszudrücken. Da sie nämlich im Allgemeinen complexe Werthe, also die Form $r(\cos\alpha + i\sin\alpha)$ haben werden, worin r positiv und α als ein Bogen unterhalb 2π angenommen werden darf, so muss

$$r^n(\cos n\alpha + i\sin n\alpha) = 1$$

sein. Daraus folgt $r = 1$, $\cos n\alpha = 1$, $\sin n\alpha = 0$, folglich ist $n\alpha$ irgend ein Vielfaches von der ganzen Peripherie 2π, etwa $2\varkappa\pi$, woraus $\alpha = \frac{2\varkappa\pi}{n}$; alle Wurzeln der Gleichung $x^n = 1$ werden also die Form

$$(\varkappa) \qquad \cos\frac{2\varkappa\pi}{n} + i\,.\,\sin\frac{2\varkappa\pi}{n}$$

haben, in welcher $\varkappa$ jede der ganzen Zahlen $0, 1, 2, 3, \ldots n-1$ sein kann, ohne dass α die Grenze 2π überschreitet.

Alle diese n Werthe sind aber auch in der That Wurzeln jener Gleichung, denn es ist:

$$\left(\cos\frac{2\varkappa\pi}{n} + i\sin\frac{2\varkappa\pi}{n}\right)^n = \cos 2\varkappa\pi + i\sin 2\varkappa\pi = 1.$$

Die Gleichung $x^n = 1$ hat hiernach n Wurzeln, welche durch den Ausdruck $(\varkappa)$ gegeben werden. Diese Wurzeln sind sämmtlich von einander verschieden; denn, wären zwei von ihnen gleich, etwa

$$\cos\frac{2\varkappa\pi}{n} + i\sin\frac{2\varkappa\pi}{n} = \cos\frac{2\varkappa'\pi}{n} + i\sin\frac{2\varkappa'\pi}{n},$$

so würde daraus $\cos\frac{2\varkappa\pi}{n} = \cos\frac{2\varkappa'\pi}{n}$, $\sin\frac{2\varkappa\pi}{n} = \sin\frac{2\varkappa'\pi}{n}$ folgen, und die Differenz $\frac{2(\varkappa-\varkappa')\pi}{n}$ müsste ein Vielfaches von 2π, oder $\varkappa - \varkappa'$ ein Vielfaches von n sein. Da aber $\varkappa$, $\varkappa'$ zwei verschiedene Zahlen aus der Reihe $0, 1, 2, \ldots n-1$ bezeichnen, deren grössere $\varkappa$ sein mag, so kann auch ihre Differenz nur eine dieser Zahlen und, da sie von Null verschieden, kein Vielfaches von n sein.

4. Wollte man statt des Ausdruckes $\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ eine andere trigonometrische Function z. B. $\cos\frac{2\pi}{n}$ den weiteren Betrachtungen zu Grunde legen, so würde man zu einer ungleich complicirteren Gleichung gelangen, als die Gleichung (1) es ist. Da wir in der Folge darauf zurückzukommen haben, wollen wir diejenige Gleichung, durch welche $\cos\frac{2\pi}{n}$ bestimmt wird, hier entwickeln. Dazu bemerken wir, dass eine Wurzel der Gleichung (1) der Einheit gleich ist, nämlich derjenige Werth des Ausdruckes $(\varkappa)$,

welcher $\varkappa = 0$ entspricht. Die übrigen Werthe sind demnach die Wurzeln der Gleichung

$$\frac{x^n - 1}{x - 1} = 0$$

oder

$$(2) \qquad x^{n-1} + x^{n-2} + \ldots + x + 1 = 0.$$

Die letztere ist eine reciproke Gleichung; setzt man daher $n - 1$, was gerade sein soll, gleich $2m$, und $x + \frac{1}{x} = y$, so nimmt sie leicht folgende Gestalt an:

$$(3) \qquad y^m + y^{m-1} - (m-1)y^{m-2} - (m-2)y^{m-3}$$
$$+ \frac{(m-2)(m-3)}{1.2} y^{m-4} + \frac{(m-3)(m-4)}{1.2} y^{m-5} - \ldots = 0.$$

Ist nun $x = \cos\frac{2\varkappa\pi}{n} + i \sin\frac{2\varkappa\pi}{n}$ eine Wurzel der Gleichung (2), so findet man, da

$$\left(\cos\frac{2\varkappa\pi}{n} + i\sin\frac{2\varkappa\pi}{n}\right)\left(\cos\frac{2\varkappa\pi}{n} - i\sin\frac{2\varkappa\pi}{n}\right)$$
$$= \cos^2\frac{2\varkappa\pi}{n} + \sin^2\frac{2\varkappa\pi}{n} = 1$$

ist,

$$\frac{1}{x} = \cos\frac{2\varkappa\pi}{n} - i\sin\frac{2\varkappa\pi}{n},$$

also ist

$$y = 2\cos\frac{2\varkappa\pi}{n}$$

eine Wurzel der Gleichung (3), und man erhält alle Wurzeln der letzteren, aber, wie leicht zu sehen ist, jede zweimal, wenn man $\varkappa$ alle seine Werthe $1, 2, 3, \ldots n-1$ durchlaufen lässt. Denn je zwei Werthen von $\varkappa$, welche sich zu n ergänzen, entspricht derselbe Werth von y, da

$$\cos\frac{2(n-\varkappa)\pi}{n} = \cos\left(2\pi - \frac{2\varkappa\pi}{n}\right) = \cos\frac{2\varkappa\pi}{n}$$

ist. Hieraus folgt, dass die Gleichung (3) die m Werthe des Ausdrucks

$$2\cos\frac{2\varkappa\pi}{n}$$

zu Wurzeln hat, welche den Werthen $\varkappa = 1, 2, 3, \ldots m$ entsprechen.

Setzt man endlich $y = 2z$ in (3) und dividirt durch 2^m, so entsteht die Gleichung;

$$(4)\qquad z^m + \tfrac{1}{2} z^{m-1} - \tfrac{1}{4}(m-1) z^{m-2} - \tfrac{1}{8}(m-2) z^{m-3} + \tfrac{1}{16} \frac{(m-2)(m-3)}{1 \,.\, 2} z^{m-4} + \ldots = 0.$$

Diese hat die m Werthe des Ausdrucks $\cos \frac{2\varkappa\pi}{n}$ für $\varkappa = 1, 2, 3, \ldots m$ zu Wurzeln, unter welchen sich auch $\cos \frac{2\pi}{n}$ befindet, und träte daher an die Stelle der Gleichung (1), wenn wir uns vornähmen, $\cos \frac{2\pi}{n}$ und nicht $\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ zu bestimmen. Wir legen jedoch die ungleich einfachere Gleichung (1) unsern weitern Betrachtungen zu Grunde.

Zweite Vorlesung.

Ein arithmetischer Hilfssatz.

1. Um nicht den Gang der nächsten Betrachtungen sogleich unterbrechen zu müssen, wollen wir hier den Beweis eines arithmetischen Satzes einschalten, den wir dabei werden anzuwenden haben.

Es sei n irgend eine positive ganze Zahl und $p, p', p'', \ldots$ die verschiedenen Primfactoren, aus welchen sie zusammengesetzt ist. Aus dieser Zahl wollen wir folgende Reihen von Zahlen ableiten, denen wir successive die Ziffern (0), (I), (II), ... zur Bezeichnung beilegen wollen:

(0) $\qquad n$

(I) $\qquad \frac{n}{p}, \frac{n}{p'}, \frac{n}{p''}, \ldots$

(II) $\qquad \frac{n}{pp'}, \frac{n}{pp''}, \frac{n}{p'p''}, \ldots$

(III) $\qquad \frac{n}{pp'p''}, \ldots$

u. s. w., bis wir in der letzten Reihe nur die eine Zahl erhalten, welche aus n durch Division mit allen verschiedenen darin enthaltenen Primfactoren entsteht. Die Divisoren all' dieser Zahlen,

sie selbst und die Einheit immer mit eingerechnet, sind offenbar keine andere Zahlen, als die in n selbst enthaltenen Divisoren. Aus ihnen sollen nun zwei Gruppen A und B gebildet werden, indem in die Gruppe A alle Divisoren der Zahlen mit gerader Ziffer, in die Gruppe B alle Divisoren der Zahlen mit ungerader Ziffer aufgenommen werden sollen. Der besagte Satz sagt dann aus:

Jeder Divisor von n findet sich gleich oft in jeder der Gruppen A und B, mit Ausnahme von n selbst, das nur einmal in der Gruppe A vorkommt.

Der letzte Theil des Satzes ist offenbar. Um auch die Richtigkeit des erstern zu erkennen, bemerke man, dass jeder Divisor d von n wenigstens einige der Primfactoren von n weniger oft enthalten wird als n selbst; es sollen deshalb diejenigen der Zahlen $p, p', p'', \ldots$, welche in d weniger oft enthalten sind als in n, und deren Anzahl gleich $\varkappa$ sei, durch

$$(\varkappa) \qquad\qquad \varpi, \varpi', \varpi'', \ldots$$

bezeichnet werden. Dann ist offenbar, dass jede Zahl, welche aus n entsteht, wenn man es durch irgend welche Combination der Zahlen $(\varkappa)$ dividirt, den Divisor d haben wird, da eine solche alle übrigen Primfactoren von n ebensooft, die Primfactoren der Reihe $(\varkappa)$ aber mindestens so oft wie d enthält; dagegen kann d nicht Divisor einer Zahl sein, welche aus n entsteht, wenn man es durch eine, auch andere Primfactoren enthaltende Combination dividirt, da eine solche diese letztern weniger oft als d enthalten würde. Hieraus folgt, dass d einmal in der Reihe (0), $\varkappa$mal in der Reihe (I), in der Reihe (II) sooft, als die Zahlen $(\varkappa)$ zu Zweien combinirt werden können, nämlich $\frac{\varkappa(\varkappa-1)}{1\,.\,2}$ mal, in der Reihe (III) sooft, als sie sich zu Dreien combiniren lassen, also $\frac{\varkappa(\varkappa-1)(\varkappa-2)}{1\,.\,2\,.\,3}$ mal als Divisor enthalten sein wird, u. s. w. Demnach findet sich, wenn man

$$(1) \quad \begin{cases} a = 1 + \frac{\varkappa(\varkappa-1)}{1\,.\,2} + \frac{\varkappa(\varkappa-1)(\varkappa-2)(\varkappa-3)}{1\,.\,2\,.\,3\,.\,4} + \ldots \\ b = \varkappa + \frac{\varkappa(\varkappa-1)(\varkappa-2)}{1\,.\,2\,.\,3} + \frac{\varkappa(\varkappa-1)(\varkappa-2)(\varkappa-3)(\varkappa-4)}{1\,.\,2\,.\,3\,.\,4\,.\,5} + \ldots \end{cases}$$

setzt und die Reihen fortsetzt, bis sie abbrechen, d in der Gruppe A genau $a$mal, und $b$mal in der Gruppe B.

Nun wird behauptet, dass $a = b$ sei. Dies folgt sofort, wenn man bemerkt, dass nach dem binomischen Lehrsatze:

$$(x-y)^\varkappa = x^\varkappa - \frac{\varkappa}{1} \cdot x^{\varkappa-1} y + \frac{\varkappa(\varkappa-1)}{1 \cdot 2} x^{\varkappa-2} y^2$$

$$- \frac{\varkappa(\varkappa-1)(\varkappa-2)}{1 \cdot 2 \cdot 3} x^{\varkappa-3} y^3 + \ldots$$

ist, woraus mit Rücksicht auf die Gleichungen (1) für $x=y=1$ sich

$$0 = a - b$$

ergiebt. — Somit ist der Satz vollständig bewiesen.

2. Bedeutet nun wieder n jede beliebige ganze Zahl und $\psi(n)$ eine irgendwie davon abhängige Grösse, sind

$$1, d, d', d'', \ldots n$$

alle Theiler von n, die Einheit und diese Zahl mit eingeschlossen, und ist endlich $f(n)$ irgend eine andere von n abhängige Grösse, welche für jedes ganzzahlige n die Gleichung:

$$(2) \qquad \psi(1) + \psi(d) + \psi(d') + \ldots + \psi(n) = f(n)$$

erfüllt, so lässt sich mit Hilfe des vorigen Satzes sehr leicht auch umgekehrt die Function $\psi(n)$ durch f-Functionen ausdrücken. Es ist nämlich

$$(3) \quad \psi(n) = f(n) - \sum_{(\mathrm{I})} f\left(\frac{n}{p}\right) + \sum_{(\mathrm{II})} f\left(\frac{n}{pp'}\right) - \sum_{(\mathrm{III})} f\left(\frac{n}{pp'p''}\right) + \cdots$$

Die Entwicklung ist soweit fortzusetzen, bis n durch alle in ihm enthaltenen verschiedenen Primfactoren dividirt wird, und den successiven Summenzeichen sind die Indices (I), (II), ... hinzugefügt, um anzudeuten, dass das Argument der Function f in ihnen resp. alle Werthe der obigen Reihen (I), (II), ... zu durchlaufen habe.

Dass diese Gleichung richtig ist, erkennt man sofort mit Hilfe des vorigen Satzes, wenn man überall die Functionen f, ihrer Definitionsgleichung (2) gemäss, durch eine Summe von ψ-Functionen ersetzt. Denn dadurch nimmt die Gleichung (3) folgende Gestalt an:

$$\psi(n) = \sum_{d:n} \psi(d) - \sum_{d:(\mathrm{I})} \psi(d) + \sum_{d:(\mathrm{II})} \psi(d) - \ldots,$$

in welcher die Summenzeichen der Reihe nach die Bedeutung haben, dass d alle Divisoren von n, alle Divisoren der Zahlen (I),

alle Divisoren der Zahlen (II) u. s. w. durchlaufen soll; man kann also einfacher schreiben:

$$\psi(n) = \sum_A \psi(d) - \sum_B \psi(d),$$

wenn in der ersten Summe d alle Zahlen aus der Gruppe A, in der zweiten alle Zahlen aus der Gruppe B durchläuft. Da aber jede von n verschiedene Zahl ebensooft in der ersten, wie in der zweiten Gruppe vorkommt, heben sich die entsprechenden ψ-Functionen in der Differenz beider Summen auf, und es bleibt von der ganzen rechten Seite der Gleichung nur das $d = n$ entsprechende Glied $\psi(n)$ der ersten Summe stehen, womit der Beweis der Formel (3) geliefert ist.

Wenn wir, um ein Beispiel zu gebrauchen, das uns bald wieder begegnen wird, statt der Gleichung (2) folgende specielle Gleichung nehmen:

$$(4) \qquad \psi(1) + \psi(d) + \psi(d') + \cdots + \psi(n) = n,$$

so findet man nach Formel (3) für $\psi(n)$ folgenden Werth:

$$\psi(n) = n - \sum_{(I)} \frac{n}{p} + \sum_{(II)} \frac{n}{pp'} - \sum_{(III)} \frac{n}{pp'p''} + \cdots$$

was einfacher offenbar auch so geschrieben werden kann:

$$(5) \qquad \psi(n) = n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p'}\right)\left(1 - \frac{1}{p''}\right)\cdots$$

Aus den Elementen der Zahlentheorie*) wird hier als bekannt vorausgesetzt, dass der die rechte Seite der Gleichung (5) bildende Werth die Function $\varphi(n)$ ausdrückt, welche die Menge der Zahlen, die kleiner als n und ohne gemeinschaftlichen Theiler mit n sind, bestimmt.

Die, durch die Gleichung (4) definirte, zahlentheoretische Function ψ ist also mit der eben bezeichneten Function φ identisch.

---

*) S. z. B. Dirichlet's Vorlesungen über Zahlentheorie, herausg. v. Dedekind. Vgl. zu dieser Vorlesung den §. 138 das.

Dritte Vorlesung.

Von den Einheitswurzeln und ihren einfachsten Eigenschaften.

1. Wir fanden in der ersten Vorlesung, dass alle Wurzeln der Gleichung:

$$x^n = 1 \tag{1}$$

durch die Formel $\cos\frac{2\varkappa\pi}{n} + i\sin\frac{2\varkappa\pi}{n}$ gegeben werden, wenn man $\varkappa$ die Werthe $0, 1, 2, 3, \ldots n-1$ durchlaufen lässt. Man bezeichnet diese Wurzeln als **Einheitswurzeln** oder, wo es darauf ankommt, den Grad der Gleichung (1) zu berücksichtigen, als **n^{te} Wurzeln der Einheit.**

Bezeichnen wir irgend eine derselben mit r, sodass $r^n = 1$ ist, so wird jede beliebige ganze Potenz von r auch eine Wurzel der Gleichung (1) sein, denn es ist:

$$(r^k)^n = (r^n)^k = 1.$$

Die unendliche Potenzenreihe $r, r^2, r^3, \ldots$ enthält demnach lauter Wurzeln der Gleichung (1) und unter ihnen mindestens eine, welche gleich Eins ist; denn, wenn keine kleinere Potenz von r der Einheit gleich wäre, so wäre es doch jedenfalls die Potenz r^n. Giebt es aber eine kleinere Potenz dieser Art, und ist r^m die kleinste unter allen, so lässt sich leicht zeigen, dass ihr Exponent m ein Theiler von n sein muss. Gesetzt nämlich, es wäre nicht der Fall, so würden m und n einen gewissen grössten gemeinschaftlichen Theiler δ haben, welcher jedenfalls $< m$ wäre. Dann kann man aber bekanntlich zwei positive oder negative ganze Zahlen p, q finden so beschaffen, dass $pm + qn = \delta$ wird. Da nun gleichzeitig $r^m = 1$ und $r^n = 1$ ist, so ergeben sich auch, mögen p und q positiv oder negativ sein, die Gleichungen

$$r^{pm} = 1, \; r^{qn} = 1 \text{ und folglich } r^{pm+qn} = r^\delta = 1,$$

d. h. m wäre nicht der niedrigste Exponent, für welchen r^m gleich Eins wird, wie doch vorausgesetzt worden ist.

Man nennt diesen kleinsten Exponenten m den Exponenten, zu welchem die Wurzel r gehört. So ergiebt sich folgender Satz:

Jede n^{te} Einheitswurzel gehört zu einem Exponenten, welcher ein Theiler von n ist.

2. Sei jetzt d ein bestimmter Divisor von n und $\psi(d)$ die Anzahl der n^{ten} Einheitswurzeln, welche zum Theiler d als Exponent gehören, sodass $\psi(d)$ gleich Null zu setzen wäre, wenn etwa keine Wurzel zu diesem Exponenten gehörte. Bemerkt man, dass nach dem eben Bewiesenen jede Wurzel der Gleichung (1) nothwendig zu einem bestimmten Divisor von n gehört, dass also die Summe aller Zahlen $\psi(d)$, wenn man diese Summe auf alle Divisoren von n bezieht, gleich der Anzahl aller n Wurzeln sein muss, so ergiebt sich, wenn $1, d, d', \ldots n$ alle Divisoren von n bedeuten, die Gleichung:

$$\psi(1) + \psi(d) + \psi(d') + \ldots + \psi(n) = n.$$

Dies ist dieselbe Gleichung, welche in der vorigen Vorlesung mit (4) bezeichnet wurde, und folglich muss $\psi(n) = \varphi(n)$ sein, wenn, wie ebendaselbst definirt worden, $\varphi(n)$ die Anzahl der Zahlen bezeichnet, welche kleiner als n und relative Primzahlen zu n sind.

Es giebt also soviel zum Exponenten n gehörige n^{te} Einheitswurzeln, als unter den Zahlen $< n$ relative Primzahlen zu n.

Da eine zum Exponenten n gehörige Wurzel der Gleichung $x^n = 1$ keiner ähnlichen Gleichung $x^k = 1$, wenn $k < n$ ist, genügen kann, so nennt man sie eine primitive Wurzel jener Gleichung und hat also folgenden Satz:

Die Gleichung $x^n = 1$ hat $\varphi(n)$ primitive Wurzeln.

3. Da dies Resultat gilt, welches auch der Grad n sei, so hat z. B. die Gleichung $x^d = 1$ $\varphi(d)$ primitive Wurzeln. Ist nun d ein Divisor von n, so ist jede primitive Wurzel ϱ dieser Gleichung eine solche n^{te} Einheitswurzel, welche zum Exponenten d gehört. Denn da $\varrho^d = 1$ ist, so ist auch $(\varrho^d)^{\frac{n}{d}} = \varrho^n = 1$, also ϱ eine n^{te} Einheitswurzel; da aber schon ϱ^d, jedoch, weil ϱ eine primitive Wurzel ist, keine kleinere Potenz der Einheit gleich wird, gehört ϱ zum Exponenten d. — Da auch umgekehrt jede zum Exponenten d gehörige Wurzel der Gleichung $x^n = 1$ offenbar eine primitive Wurzel von $x^d = 1$ ist, da sie zwar dieser Gleichung, aber keiner ähnlichen von kleinerem Grade genügt, so stimmen die n^{ten} Einheitswurzeln, welche zum Exponenten d gehören, mit den primitiven Wurzeln der Gleichung $x^d = 1$ überein, und es gilt der Satz:

Es giebt $\varphi(d)$ n^{te} Einheitswurzeln, welche zum Divisor d von n als Exponent gehören. Dieselben sind die primitiven Wurzeln der Gleichung $x^d = 1$.

4. Bezeichnet r irgend eine primitive Wurzel der Gleichung (1), so können alle ihre Wurzeln durch die folgende Reihe von Potenzen dargestellt werden:

$$(2) \qquad r, r^2, r^3, \ldots r^n.$$

In der That: erstens sind diese sämmtlich Wurzeln der Gleichung (1). Aber sie sind auch alle unter einander verschieden; wären nämlich r^h und r^k einander gleich, unter h und k zwei verschiedene Zahlen der Reihe $1, 2, 3, \ldots n$ verstanden, von welchen h die grössere sei, so ergäbe sich $r^{h-k} = 1$, während $h - k < n$ ist, gegen die Voraussetzung, nach welcher r eine primitive Wurzel der Gleichung (1) ist.

Unter den Wurzeln (2) gehören diejenigen zum Exponenten d, deren Exponenten mit n den grössten gemeinschaftlichen Divisor $\delta = \frac{n}{d}$ haben. Denn es sei r^h eine solche Potenz, der Art dass man $h = h'\delta$, $n = d\delta$ setzen und dabei unter h' und d zwei relative Primzahlen verstehen kann. Ist μ der Exponent, zu welchem r^h gehört, so ist $r^{h\mu} = 1$. Da aber r selber zum Exponenten n gehört und der Gleichung $x^{h\mu} = 1$ genügen soll, muss $h\mu$ nach dem Satze in Nr. 1 ein Vielfaches von n oder $h'\mu$ ein Vielfaches von d sein, und weil h' zu d prim ist, muss μ ein Vielfaches von d sein. Nun ist aber schon

$$(r^h)^d = (r^n)^{h'} = 1,$$

also ist der kleinste Werth von μ, für welchen $r^{h\mu}$ gleich Eins werden kann, der Werth $\mu = d$.

Zusatz: Unter den Wurzeln (2) sind diejenigen primitive Wurzeln, deren Exponenten relative Primzahlen zu n sind. Denn für diese ist $\delta = \frac{n}{d} = 1$, also $d = n$.

5. Da nach der vorigen Nummer die Wurzeln der Gleichung (1) durch die Reihe (2) dargestellt werden können, so kann man mittels eines bekannten algebraischen Satzes den Ausdruck $x^n - 1$ nach folgender Gleichung in lineare Factoren zerlegen:

$$x^n - 1 = (x - r)(x - r^2) \ldots (x - r^n).$$

Denken wir uns auf der rechten Seite dieser Gleichung immer

diejenigen Factoren zu einem besonderen Producte zusammengefasst, in welchen die Wurzeln zu demselben Divisor d von n als Exponent gehören, und bezeichnen das dem Divisor d entsprechende Product mit $F_d(x)$, so ist nach dem Satze in Nr. 3 klar, dass die Gleichung $F_d(x) = 0$ die primitiven Wurzeln der Gleichung $x^d = 1$ zu Wurzeln hat. Andererseits kann $x^n - 1$, was wir kurz mit $f_n(x)$ oder, wo es auf den Werth von x nicht ankommt, noch einfacher durch $f(n)$ bezeichnen wollen, unter der Form des Products $\Pi F_d(x)$ dargestellt werden, welches sich auf alle Divisoren d von n bezieht, was wir ausdrücken wollen, indem wir schreiben:

$$f_n(x) = \prod_{d:n} F_d(x).$$

Da nun die Wurzeln der Gleichung (1) oder der Gleichung $f_n(x)=0$ mit den Wurzeln aller Gleichungen $F_d(x) = 0$ zusammenfallen müssen, liefert diese Gleichung zunächst den Satz:

Die Wurzeln der Gleichung (1) stimmen mit den primitiven Wurzeln aller Gleichungen $x^d = 1$ überein, welche man erhält, wenn für d successive alle Theiler von n gesetzt werden, diese Zahl und die Einheit mit eingeschlossen.

Aus derselben Gleichung kann man aber auch den Ausdruck für $F_n(x)$ bestimmen. Nimmt man nämlich von beiden Seiten die Logarithmen, so erhält man:

$$\log . f(n) = \sum_{d:n} \log . F_d(x),$$

eine Gleichung genau von der Art wie die Gleichung (2) der vorigen Vorlesung, denn die Summation erstreckt sich über alle Theiler d von n. Bezeichnen daher $p, p', p'', \ldots$ die verschiedenen in n enthaltenen Primfactoren, so erhält man sofort für $\log . F_n(x)$ folgenden Ausdruck:

$$\log . F_n(x) = \log . f(n) - \sum_{(I)} \log . f\left(\frac{n}{p}\right) + \sum_{(II)} \log . f\left(\frac{n}{pp'}\right) - \cdots$$

oder, indem man von den Logarithmen zu den Grössen selbst zurückkehrt,

$$(3)\qquad F_n(x) = \frac{f(n)\cdot \prod\limits_{(II)} f\left(\frac{n}{pp'}\right)\cdots}{\prod\limits_{(I)} f\left(\frac{n}{p}\right)\cdot \prod\limits_{(III)} f\left(\frac{n}{pp'p''}\right)\cdots}.$$

Die Ausdehnung der einzelnen Summen resp. Producte ist durch die Bestimmungen in Nr. 2 der vorigen Vorlesung gegeben.

Nun ist $F_n(x)$ eine ganze Function von x vom Grade $\varphi(n)$, denn die Gleichung

$$(4)\qquad F_n(x) = 0$$

enthält als Wurzeln alle primitive n^{te} Einheitswurzeln. Es heben sich also die Nenner in dem Ausdrucke (3) durch Division heraus; bei der Division können jedoch keine Brüche eingeführt werden, da die Coëfficienten der höchsten Potenzen von x in den einzelnen Factoren, der Bedeutung des Zeichens f gemäss, sämmtlich der Einheit gleich sind.

Demnach ist $F_n(x)$ eine ganze Function von x vom Grade $\varphi(n)$ mit ganzzahligen Coëfficienten, deren höchster gleich Eins ist.

Nehmen wir speciell n als Primzahlpotenz an, $n = p^a$, so wird die Gleichung für die primitiven Wurzeln:

$$\frac{x^{p^a} - 1}{x^{p^{a-1}} - 1} = 0$$

oder

$$(5)\qquad x^{p^{a-1}(p-1)} + x^{p^{a-1}(p-2)} + \ldots + x^{p^{a-1}} + 1 = 0.$$

Wenn endlich $n = p$ also $a = 1$ ist, erhält man für die Gleichung, welcher die primitiven p^{ten} Wurzeln angehören, die folgende:

$$(6)\qquad \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1 = 0.$$

Es sind demnach, wenn p eine Primzahl ist, alle Wurzeln der Gleichung $x^p = 1$ mit Ausnahme der einzigen, welche der Einheit gleich ist, primitive Wurzeln derselben. Die Verbindung dieses Resultates mit dem ersten Satze in Nr. 4 ergiebt den folgenden Satz:

Bezeichnet r irgend eine Wurzel der Gleichung (6), so können alle ihre Wurzeln durch die Reihe von Potenzen:

(7) $$r,\ r^2,\ r^3,\ \ldots\ r^{p-1}$$

dargestellt werden.

6. Da man nach Nr. 4 sämmtliche Wurzeln der Gleichung (1), welches auch n sein mag, erhalten kann, wenn man eine primitive Wurzel derselben kennt, so kommt die Aufgabe der Kreistheilung auf die Auffindung einer primitiven n^{ten} Einheitswurzel zurück. Wenn n eine zusammengesetzte Zahl, etwa

$$n = p^\alpha \,.\, p'^{\alpha'} \,.\, p''^{\alpha''} \ldots$$

ist, worin $p,\ p',\ p'',\ \ldots$ verschiedene ungerade Primzahlen bedeuten, so lässt sich die neue Aufgabe noch weiter vereinfachen, denn es besteht der Satz: Sind $u,\ v,\ w,\ \ldots$ primitive Wurzeln der Gleichungen:

$$x^{p^\alpha} = 1, \quad x^{p'^{\alpha'}} = 1, \quad x^{p''^{\alpha''}} = 1, \ \ldots$$

resp., so ist $r = u\,.\,v\,.\,w \ldots$ eine primitive Wurzel der Gleichung $x^n = 1$.

In der That, weil n durch jede der Zahlen $p^\alpha,\ p'^{\alpha'},\ p''^{\alpha''}, \ldots$ theilbar ist, so ist jede der Potenzen $u^n,\ v^n,\ w^n,\ \ldots$ folglich auch r^n gleich Eins, jedenfalls also r eine Wurzel der Gleichung $x^n=1$. Gehörte diese Wurzel nun nicht zum Exponenten n, sondern zu einem Divisor d von n, so würde in diesem wenigstens eine der Primzahlen $p,\ p',\ p'',\ \ldots$ weniger oft als in n enthalten sein, z. B. die Primzahl p nur β mal, während $\beta < \alpha$. Da alsdann $p^\beta \,.\, p'^{\alpha'} \,.\, p''^{\alpha''} \ldots$ jedenfalls durch d theilbar ist, so ergiebt sich aus der vorausgesetzten Gleichung $r^d = 1$ die andere:

$$r^{p^\beta . p'^{\alpha'} . p''^{\alpha''} \cdots} = 1,$$

welche sich zunächst auf die folgende:

$$u^{p^\beta . p'^{\alpha'} . p''^{\alpha''} \cdots} = 1$$

reducirt; daraus und in Verbindung mit der Gleichung $u^{p^\alpha} = 1$ folgt aber, wenn man, was möglich ist*), zwei ganze Zahlen x, y der Gleichung

$$x \,.\, p^\alpha + y \,.\, p^\beta p'^{\alpha'} p''^{\alpha''} \ldots = p^\beta$$

gemäss bestimmt, die nachstehende Gleichung:

*) Denn die Zahlen p^α und $p^\beta \,.\, p'^{\alpha'} p''^{\alpha''} \ldots$ haben den grössten gemeinsamen Theiler p^β.

$$u^{p^\beta} = 1,$$

welche unmöglich ist, da u zum Exponenten p^α gehören sollte.

Nach diesem Satze kommt die Theilung der Kreisperipherie in eine Anzahl n gleicher Theile in dem Falle, wo n eine beliebig zusammengesetzte Zahl ist, offenbar auf den Fall zurück, wo die Zahl n eine Potenz einer ungeraden Primzahl, $n = p^\alpha$, ist.

In dem einfachsten Falle, in welchem der Kreis in p gleiche Theile getheilt werden soll, wird die Aufgabe als gelöst anzusehen sein, wenn man eine primitive Wurzel der Gleichung $x^p = 1$ d. i. irgend eine Wurzel r der Gleichung (6) gefunden hat. Im Folgenden soll dieser Fall fast ausschliesslich behandelt werden, hauptsächlich der Einfachheit wegen, zudem aber auch, weil der allgemeinere, wo $n = p^\alpha$ ist, zu keinen wesentlich neuen Betrachtungen Anlass giebt*). Nur ausnahmsweise werden wir auf den allgemeinen Fall wieder zurückkommen. Die Gleichung (6) soll hinfort als Kreistheilungsgleichung bezeichnet werden.

7. Zum Schluss dieser Vorlesung mögen einige einfache Bemerkungen Platz finden, welche sich noch auf den Fall einer beliebigen ganzen Zahl n beziehen.

1) Da jede positive ganze Zahl m gleich $an + b$ gesetzt werden kann, wo b positiv und kleiner als n ist, so ergiebt sich

$$r^m = r^{an} \cdot r^b = r^b$$

d. h. der Exponent einer Potenz von r kann stets durch seinen kleinsten positiven Rest (mod. n) ersetzt werden. Hieraus folgt unmittelbar

$$r^m = r^{m'}$$

wenn

$$m \equiv m' \quad (\text{mod. } n)$$

ist, und umgekehrt. Man kann r auch mit negativem Exponenten, r^{-m}, nehmen, wenn man darunter die Potenz r^b versteht, deren Exponent b der kleinste positive Rest von $-m$ (mod. n) ist. Dies wird in der Folge vielfach benutzt werden.

2) Nach Nr. 4 giebt jede primitive n^{te} Einheitswurzel r durch ihre n ersten Potenzen alle übrigen Einheitswurzeln desselben Grades. Bezeichnet ferner $\varkappa$ irgend eine zu n relativ prime Zahl,

---

*) Vgl. Gauss disqu. arithm. art. 336.

so ist (nach dem Zusatze ebendas.) $r^\varkappa$ ebenfalls eine primitive Wurzel. Daher ergiebt die Reihe von Potenzen:

$$r^\varkappa,\ r^{2\varkappa},\ r^{3\varkappa},\ \ldots\ r^{(n-1)\varkappa},\ r^{n\varkappa}$$

wieder alle n^{ten} Einheitswurzeln, stimmt also, von der Reihenfolge abgesehen, mit der andern Reihe:

$$r,\ r^2,\ r^3,\ \ldots\ r^{n-1},\ r^n$$

völlig überein. Hierbei sind die letzten Glieder beider Reihen einander gleich, da sie den Werth Eins haben. Dies Resultat lässt sich demnach folgendermassen aussprechen:

Wenn $\varkappa$ eine zu n relativ prime Zahl bedeutet, so ist die Substitution von $r^\varkappa$ statt r in der Reihe

$$r,\ r^2,\ r^3,\ \ldots\ r^{n-1}$$

mit einer gewissen Permutation dieser Grössen gleichbedeutend.

3) Da hiernach die Summen:

$$r^\varkappa + r^{2\varkappa} + r^{3\varkappa} + \ldots + r^{n\varkappa}$$
$$r + r^2 + r^3 + \ldots + r^n$$

einander gleich, nämlich gleich der Summe aller Wurzeln der Gleichung (1) sind, sobald $\varkappa$ eine zu n relativ prime Zahl bedeutet, so ergeben sie sich nach bekanntem Satze der Algebra gleich dem negativen Coëfficienten der Potenz x^{n-1} in der Gleichung (1) d. h. gleich Null, und man findet, mit Rücksicht darauf, dass $r^n = r^{\varkappa n} = 1$ ist, folgende Beziehung:

$$(8) \qquad 1 + r^\varkappa + r^{2\varkappa} \ldots + r^{(n-1)\varkappa} = 0.$$

Diese Gleichung folgt auch, sogar in noch grösserer Allgemeinheit aus der folgenden:

$$1 + r^\varkappa + r^{2\varkappa} + \ldots + r^{(n-1)\varkappa} = \frac{r^{n\varkappa} - 1}{r^\varkappa - 1},$$

welche lehrt, dass die Gleichung (8) allgemeiner für jeden Werth von $\varkappa$ erfüllt ist, welcher durch n nicht theilbar ist, denn für jeden solchen Werth von $\varkappa$ wird der Zähler des Bruches gleich Null, während der Nenner von Null verschieden ist, sobald r als primitive n^{te} Einheitswurzel vorausgesetzt wird.

Vierte Vorlesung.

Hilfssätze über Congruenzen. — Die primitiven Wurzeln (mod. p).

1. Die Methode, welche wir im Folgenden zur Auflösung der Kreistheilungsgleichung d. i. der Gleichung $\frac{x^p - 1}{x - 1} = 0$ auseinanderzusetzen haben, ruht wesentlich auf zwei verschiedenen Grundlagen, die jedoch Beide ein- und demselben weiteren Gebiete der Arithmetik, der Lehre von den höheren Congruenzen, angehören. Dies sind einerseits die Eigenschaften der sogenannten primitiven Wurzeln vom Modulus p, andererseits die Irreductibilität der Kreistheilungsgleichung. Ehe wir zu ihrer speciellen Betrachtung übergehen können, müssen hier einige einfache Fundamentalsätze jener Theorie, deren wir bedürfen werden, bewiesen werden.

Wir beginnen mit einer Definition, welche den elementaren Begriff der Congruenzen erweitert:

Zwei ganze Functionen von x:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$$
$$\varphi(x) = b_0 x^n + b_1 x^{n-1} + \dots + b_{n-1} x + b_n$$

mit ganzzahligen Coëfficienten sollen (mod. p) congruent heissen, in Zeichen:

$$f(x) \equiv \varphi(x) \quad (\text{mod. } p),$$

wenn die Coëfficienten gleich hoher Potenzen (mod. p) einander congruent sind, wenn also für jeden Index i die Congruenz $a_i \equiv b_i$ (mod. p) besteht.

Man kann die Functionen von demselben Grade annehmen, indem man im entgegengesetzten Falle die fehlenden Potenzen mit dem Coëfficienten Null hinzufügt.

Hiernach wird eine Function $f(x)$ congruent Null heissen (mod. p), wenn jeder ihrer Coëfficienten durch p theilbar ist.

Ist p eine Primzahl, so besteht folgender Satz*): Das Product zweier ganzer und ganzzahliger Functionen $f(x)$

*) Vgl. hierzu Eisenstein's Abhandlung in Crelle's Journal Bd. 39, pag. 167 und 168.

und $\varphi(x)$ kann nur dann congruent Null sein (mod. p), wenn es einer der Factoren ist.

Denn, nehmen wir das Gegentheil an, so muss in jeder der Functionen $f(x)$ und $\varphi(x)$ mindestens ein Coëfficient durch p nicht theilbar sein. Sei, vom letzten an gerechnet, a_{n-i} der erste nicht durch p theilbare Coëfficient in $f(x)$, b_{n-k} der erste in $\varphi(x)$, sodass alle Coëfficienten mit grösserem Index durch p theilbar sind. Dann ist leicht zu sehen, dass der Coëfficient von x^{i+k} im entwickelten Producte $f(x) \,.\, \varphi(x)$ gleich

$$a_{n-i} \,.\, b_{n-k} + a_{n-i+1} \,.\, b_{n-k-1} + \ldots + b_{n-k+1} \,.\, a_{n-i-1} + \ldots$$

d. h. gleich $a_{n-i} \,.\, b_{n-k}$ plus einer Reihe von Gliedern ist, welche nach der Voraussetzung durch p theilbar sind, er ist also congruent $a_{n-i} \,.\, b_{n-k}$ (mod. p). Dieses Product kann aber, wenn p eine Primzahl ist, nicht durch p theilbar sein, da es keiner der Factoren ist, und folglich können auch in dem Producte $f(x) \,.\, \varphi(x)$ nicht alle Coëfficienten durch p theilbar sein, wie es doch sein soll; also ist unsere Annahme unzulässig.

2. Auf diesem Satze beruht ein anderer sehr wichtiger Satz, welchen zuerst Gauss in den Disquis. arithm. Nr. 42 bewiesen hat. Denselben sprechen wir folgendermassen aus:

Wenn eine ganze Function

$$f(x) = x^{m+n} + c_1 x^{m+n-1} + \ldots + c_{m+n-1} \,.\, x + c_{m+n}$$

mit ganzzahligen Coëfficienten, deren höchster gleich Eins ist, nicht in das Product zweier ganzer Functionen:

$$\varphi(x) = x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m$$
$$\psi(x) = x^n + b_1 x^{n-1} + \ldots + b_{n-1} x + b_n$$

mit ganzzahligen Coëfficienten zerlegbar ist, so ist sie es auch nicht in das Product von zwei solchen ganzen Functionen mit rationalen Coëfficienten. — In der That, wäre solche Zerlegung möglich, also

$$f(x) = \varphi(x) \,.\, \psi(x),$$

so bringe man die Coëfficienten in $\varphi(x)$ auf ihren Generalnenner α, diejenigen von $\psi(x)$ auf ihren Generalnenner β und multiplicire mit denselben die Gleichung; setzt man allgemein $a_i = \frac{\alpha_i}{\alpha}$, $b_i = \frac{\beta_i}{\beta}$ und $\alpha\beta = C$, so entsteht die Gleichung:

$$C \,.\, f(x) = \varphi'(x) \,.\, \psi'(x)$$

worin die Functionen:

$$\varphi'(x) = \alpha x^m + \alpha_1 x^{m-1} + \ldots + \alpha_{m-1} x + \alpha_m$$
$$\psi'(x) = \beta x^n + \beta_1 x^{n-1} + \ldots + \beta_{n-1} x + \beta_n$$

ganzzahlige Coëfficienten haben. Nach dem vorigen Satze muss nun jede in C aufgehende Primzahl p alle Coëfficienten entweder von $\varphi'(x)$ oder von $\psi'(x)$ theilen, kann also fortgehoben werden, und darauf entsteht eine neue Gleichung von der Form:

$$f(x) = \varphi''(x) \,.\, \psi''(x),$$

worin $\varphi''(x)$, $\psi''(x)$ ganze Functionen mit ganzzahligen Coëfficienten sind, deren höchste gleich Eins sein müssen, da ihr Product dem höchsten Coëfficienten von $f(x)$, also der Einheit gleich ist. Eine solche Zerlegung von $f(x)$ widerstreitet aber der Voraussetzung.

3. Sei ferner

$$f(x) = x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m = 0$$

eine Gleichung mit ganzzahligen Coëfficienten und den Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_m$, und p eine ungerade Primzahl, wie fortan überhaupt angenommen werden soll. Für spätere Untersuchungen ist es wichtig, diejenige Gleichung zu betrachten, deren Wurzeln die p^{ten} Potenzen von den Wurzeln der gegebenen sind. Um zunächst diese Gleichung zu bilden, bemerke man, dass, wenn z einen beliebigen Werth bedeutet, die Gleichung

$$x^m + a_1 z x^{m-1} + a_2 z^2 x^{m-2} + \ldots + a_{m-1} z^{m-1} x + a_m z^m = 0$$

nach einem bekannten Satze der Algebra die Wurzeln

$$z\alpha_1, \; z\alpha_2, \; \ldots \; z\alpha_m$$

besitzt. Setzt man demnach successive z den Potenzen $r, r^2, \ldots r^{p-1}$ gleich, während r eine primitive p^{te} Einheitswurzel bedeutet, so werden die folgenden Gleichungen:

$$\left.\begin{array}{l}
x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m = 0 \\
x^m + a_1 r x^{m-1} + \ldots + a_{m-1} r^{m-1} x + a_m r^m = 0 \\
x^m + a_1 r^2 x^{m-1} + \ldots + a_{m-1} r^{2(m-1)} x + a_m r^{2m} = 0 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
x^m + a_1 r^{p-1} x^{m-1} + \ldots + a_{m-1} r^{(p-1)(m-1)} . x + a_m r^{(p-1)m} = 0
\end{array}\right\} (R)$$

resp. die Wurzeln haben:

$$\left.\begin{array}{lllll} \alpha_1, & \alpha_2, & \alpha_3, & \ldots & \alpha_m \\ r\alpha_1, & r\alpha_2, & r\alpha_3, & \ldots & r\alpha_m \\ r^2\alpha_1, & r^2\alpha_2, & r^2\alpha_3, & \ldots & r^2\alpha_m \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ r^{p-1}\alpha_1, & r^{p-1}\alpha_2, & r^{p-1}\alpha_3, & \ldots & r^{p-1}\alpha_m. \end{array}\right\} (r)$$

Das Product $\varphi(x) = 0$ dieser Gleichungen enthält demnach das ganze System (r) von Wurzeln. Aus der Gleichung:

$$(x - 1)(x - r)(x - r^2) \ldots (x - r^{p-1}) = x^p - 1,$$

welche aus der ersten Gleichung in Nr. 5 der vorigen Vorlesung hervorgeht, wenn p für n und für r^p sein Werth 1 gesetzt wird, folgt aber, indem x durch $\frac{x}{\alpha}$ ersetzt und mit α^p multiplicirt wird,

$$(x - \alpha)(x - r\alpha)(x - r^2\alpha) \ldots (x - r^{p-1}\alpha) = x^p - \alpha^p.$$

Daher ist offenbar $\varphi(x)$ nichts Anderes als das Product:

$$(x^p - \alpha_1{}^p)(x^p - \alpha_2{}^p) \ldots (x^p - \alpha_m{}^p),$$

und folglich erhält man aus der Gleichung $\varphi(x) = 0$ die gesuchte, indem man einfach x^p durch x ersetzt, denn so geht dieselbe in die folgende über:

$$(x - \alpha_1{}^p)(x - \alpha_2{}^p) \ldots (x - \alpha_m{}^p) = 0,$$

welche die p^{ten} Potenzen der Wurzeln der gegebenen Gleichung zu Wurzeln hat. Wir bezeichnen diese Gleichung in entwickelter Gestalt durch:

$$F(x) = x^m + b_1 x^{m-1} + \ldots + b_{m-1} x + b_m = 0.$$

4. Diese Gleichung steht nun mit der gegebenen in einer merkwürdigen Congruenzbeziehung (mod. p), welche wir ableiten müssen. — Nach der zweiten Bemerkung in Nr. 7 der vorigen Vorlesung ist die Substitution von $r^\varkappa$ an Stelle von r in der Reihe $r, r^2, r^3, \ldots r^{p-1}$, wenn $\varkappa$ nicht durch p theilbar ist, gleichbedeutend mit einer gewissen Permutation dieser Grössen. Dies vorausgeschickt, bemerken wir, dass das Product $\varphi(x)$ offenbar symmetrisch ist in Beziehung auf die letzteren, also ungeändert bleibt, wie man dieselben auch unter einander permutirt z. B. bei jeder Substitution einer Potenz $r^\varkappa$ an Stelle von r. Denkt man sich andererseits das Product $\varphi(x)$ entwickelt und nach Potenzen von r geordnet und beachtet, dass jede Potenz r^m, bei welcher $m > p$ ist, nach der ersten Bemerkung a. a. O. durch eine an-

dere ersetzt werden kann, bei welcher der Exponent kleiner als p ist, so nimmt das entwickelte Product $\varphi(x)$ die Gestalt an:

$$\varphi(x) = \xi_0 + \xi_1 r + \xi_2 r^2 + \ldots + \xi_{p-1} \cdot r^{p-1},$$

in welcher die Coëfficienten ξ ganze und ganzzahlige Functionen von x sein müssen. Da, wie bemerkt, dieses Product bei jeder Substitution von $r^\varkappa$ anstatt r, bei welcher $\varkappa$ durch p nicht theilbar ist, unverändert bleibt, ergeben sich, wenn successive $\varkappa = 2, 3, \ldots p-1$ gesetzt wird, für $\varphi(x)$ noch folgende Ausdrücke:

$$\varphi(x) = \xi_0 + \xi_1 r^2 + \xi_2 r^4 + \ldots + \xi_{p-1} \cdot r^{2(p-1)}$$

$$\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot$$

$$\varphi(x) = \xi_0 + \xi_1 r^{p-1} + \xi_2 r^{2(p-1)} + \ldots + \xi_{p-1} \cdot r^{(p-1)(p-1)},$$

welche, zu jenem ersten addirt, die Gleichung liefern:

$$(p-1)\,\varphi(x) = (p-1)\,\xi_0 + \xi_1 (r + r^2 + \ldots + r^{p-1})$$
$$+ \xi_2 (r^2 + r^4 + \ldots + r^{2(p-1)}) + \ldots + \xi_{p-1} (r^{p-1} + r^{2(p-1)} + \ldots + r^{(p-1)(p-1)}),$$

oder, da die Factoren von $\xi_1, \xi_2, \ldots \xi_{p-1}$ nach der Gleichung (8) der vorigen Vorlesung den gemeinsamen Werth -1 haben,

$$(p-1)\,\varphi(x) = p\xi_0 - (\xi_0 + \xi_1 + \xi_2 + \ldots + \xi_{p-1}).$$

Die in Klammern stehende Grösse ergiebt sich aber aus $\varphi(x)$, indem man r gleich Eins setzt, wodurch alle Factoren von $\varphi(x)$ gleich $f(x)$ werden, sie ist also gleich $f(x)^p$. Fasst man ausserdem die vorstehende Gleichung als eine Congruenz (mod. p) auf, so zeigt sich, dass

$$(1) \qquad \varphi(x) \equiv f(x)^p \pmod{p}$$

ist.

5. Hier mag eine Bemerkung eingeschaltet werden, von welcher im Folgenden ein ausgedehnter Gebrauch gemacht werden wird. Ist

$$F(x) = A_0 x^m + A_1 x^{m-1} + \ldots + A_{m-1} x + A_m$$

eine ganze Function von x mit ganzzahligen Coëfficienten, und p eine (ungerade) Primzahl, so lehrt der polynomische Satz, dass die Entwicklung der p^{ten} Potenz von $F(x)$ ausser den p^{ten} Potenzen der einzelnen Glieder nur solche Glieder enthält, deren Coëfficienten durch p theilbar sind. In der That, alle, von den p^{ten} Potenzen der einzelnen Glieder verschiedenen Glieder der Entwicklung haben

die sogenannten Polynomialcoëfficienten zu Factoren; diese sind natürlich ganze Zahlen und haben die allgemeine Form:

$$\frac{1 . 2 . 3 \ldots p}{1 . 2 \ldots \varkappa . 1 . 2 \ldots \varkappa' \ldots 1 . 2 \ldots \varkappa^{(m)}},$$

worin $\varkappa, \varkappa', \ldots \varkappa^{(m)}$ $m + 1$ positive ganze Zahlen sind, deren Summe gleich p. Jeder Ausdruck dieser Art aber ist durch p theilbar, da alle im Nenner enthaltenen Zahlen kleiner als die Primzahl p sind, diese also bei der Division als Factor bestehen bleibt. Man darf daher setzen:

(2) $F(x)^p = A_0{}^p x^{mp} + A_1{}^p x^{(m-1)p} + \ldots + A_{m-1}{}^p x^p + A_m{}^p + p . F_1(x)$,

wo $F_1(x)$ eine gewisse ganze Function von x mit ganzzahligen Coëfficienten bezeichnet, oder, wenn wir die Definition einander (mod. p) congruenter Functionen benutzen,

(3) $F(x)^p \equiv A_0{}^p x^{mp} + A_1{}^p x^{(m-1)p} + \ldots + A_{m-1}{}^p x^p + A_m{}^p$ (mod. p).

Kehren wir jetzt zur Congruenz (1) wieder zurück, so können wir ihr folgende Gestalt geben:

$$\varphi(x) \equiv x^{mp} + a_1{}^p . x^{(m-1)p} + \ldots + a_{m-1}{}^p x^p + a_m{}^p \text{ (mod. } p)$$

oder endlich, indem man in dieser, für jedes x bestehenden Congruenz x^p durch x ersetzen darf, wodurch dann $\varphi(x)$ in $F(x)$ übergeht:

(4) $$x^m + b_1 x^{m-1} + \ldots + b_{m-1} x + b_m \equiv x^m + a_1{}^p x^{m-1} + \ldots + a_{m-1}{}^p x + a_m{}^p.$$

6. Ehe wir dieses Resultat in seiner wahren Bedeutung erkennen können, müssen wir einen wichtigen speciellen Fall desselben vorausschicken. Reducirt sich nämlich die Gleichung $f(x) = 0$ auf die folgende:

$$(x - 1)^m = x^m - m x^{m-1} + \frac{m(m-1)}{1 . 2} x^{m-2} + \ldots = 0,$$

so wird $F(x)$ von $f(x)$ nicht verschieden sein, da jede Wurzel der vorigen Gleichung ebenso wie ihre p^{te} Potenz der Einheit gleich ist. In diesem Falle nimmt also die allgemeine Congruenz (4) die besondere Form an:

$$x^m - m x^{m-1} + \ldots \equiv x^m - m^p . x^{m-1} + \ldots \text{ (mod. } p),$$

woraus sich durch Vergleichung der Coëfficienten von x^{m-1} die wichtige Congruenz ergiebt:

(5) $$m^p \equiv m \text{ (mod. } p).$$

Jede Zahl ist also ihrer p^{ten} Potenz (mod. p) congruent, wenn p eine (ungerade) Primzahl ist.

Wenn m nicht durch p theilbar ist, kann man die vorige Congruenz bekanntlich durch den gemeinsamen Factor m beider Seiten theilen und erhält dann:

$$m^{p-1} \equiv 1 \pmod{p}$$

d. h. den berühmten Fermat'schen Satz: die $(p-1)^{te}$ Potenz jeder durch p nicht theilbaren Zahl giebt, durch p getheilt, den Rest Eins, wenn p eine (ungerade) Primzahl*) ist.

Mit Rücksicht auf die Congruenz (5) können wir die Relationen (2) und (3) auch folgendermassen schreiben:

$$F(x)^p = A_0 x^{mp} + A_1 x^{(m-1)p} + \ldots + A_{m-1} x^p + A_m + p \cdot f'(x)$$

wenn $f'(x)$ eine gewisse ganze Function von x mit ganzzahligen Coëfficienten bedeutet, oder kürzer:

$$F(x)^p = F(x^p) + p \cdot f'(x) \tag{6}$$

oder als Congruenz:

$$F(x)^p \equiv F(x^p) \pmod{p}. \tag{7}$$

Wendet man endlich das in (5) erhaltene Resultat auf die Congruenz (4) am Schlusse der vorigen Nr. an, so ergiebt sich der interessante Satz: Die ganze Function, welche die p^{ten} Potenzen von den Wurzeln einer andern ganzen Function zu Wurzeln hat, ist, wenn p eine ungerade Primzahl bedeutet, dieser ganzen Function (mod. p) congruent**).

7. Wenn in einer Function $f(x)$ die ganzzahligen Coëfficienten nicht sämmtlich durch p theilbar sind, so besteht die Congruenz $f(x) \equiv 0 \pmod{p}$ nicht mehr identisch, es entsteht vielmehr die Aufgabe, diejenigen ganzzahligen Werthe von x zu finden, welche ihr Genüge leisten. Jeder Werth von x dieser Art heisst eine Wurzel der Congruenz. Wenn $x = \alpha$ eine solche ist, so wird jeder Werth von x, welcher dem α congruent ist (mod. p), offenbar auch eine Wurzel sein; alle diese unendlich vielen Wur-

*) Offenbar gilt der Satz auch für $p = 2$, jedoch bedürfen wir im Folgenden dieses Falles nicht.

**) Vergl. hiezu: in Crelle's J. Bd. 31 Schoenemann, Grundzüge einer allgemeinen Theorie der höheren Congruenzen, §. 13.

zeln sieht man aber als eine einzige Congruenzwurzel an, indem man sagt, die Congruenz habe die Wurzel $x \equiv \alpha \pmod{p}$.

Ist $f(x) \equiv \varphi(x) \pmod{p}$, so haben die beiden Congruenzen $f(x) \equiv 0$ und $\varphi(x) \equiv 0 \pmod{p}$ dieselben Wurzeln, da jeder Werth von x, welcher die eine Function durch p theilbar macht, auch die andere durch p theilbar machen muss.

Es ist ein Hauptsatz, dass die Anzahl incongruenter Wurzeln einer Congruenz nicht grösser als ihr Grad sein kann. Dabei versteht man unter Grad der Congruenz den Exponenten derjenigen höchsten Potenz von x, deren Coëfficient durch p nicht theilbar ist. Ist nun

$$f(x) = a_0 x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m \equiv 0 \pmod{p}$$

die gegebene Congruenz, m ihr Grad, also a_0 nicht theilbar durch p, so kann man stets $a_0 = 1$ voraussetzen; denn im entgegengesetzten Falle lässt sich bekanntlich eine, durch p nicht theilbare, ganze Zahl α_0 finden von der Art, dass $a_0 \alpha_0 \equiv 1 \pmod{p}$ ist, und da die Wurzeln der Congruenz dieselben bleiben müssen, wenn man diese mit der constanten Zahl α_0 multiplicirt, so führt man dadurch die Congruenz in eine andere äquivalente über, in welcher der Coëfficient der höchsten Potenz gleich Eins ist. Nehmen wir also von vornherein $a_0 = 1$ an.

Um nun den Satz zu beweisen, setzen wir ihn für jede Function bis zum $(m-1)^{ten}$ Grade als bewiesen voraus, und zeigen sodann seine Richtigkeit auch für die Functionen des m^{ten} Grades; so wird seine allgemeine Gültigkeit erhellen, da jede Congruenz ersten Grades, welche nach dem eben Gesagten die Form $x + a_1 \equiv 0 \pmod{p}$ annimmt, nur eine Wurzel $x \equiv -a_1 \pmod{p}$ haben kann. Hat aber die Congruenz:

$$x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m \equiv 0 \pmod{p}$$

mindestens m incongruente Wurzeln, so seien diese $\alpha_1, \alpha_2, \ldots \alpha_m$; man hat dann algebraisch:

$$x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_m) + \varphi(x),$$

worin $\varphi(x)$ eine gewisse ganze Function von x, höchstens vom Grade $m-1$ ist, mit ganzzahligen Coëfficienten, welche, wie leicht zu zeigen, durch p theilbar sind; denn, da sowohl die linke Seite der Gleichung, als auch das Product auf der rechten für die m incongruenten Werthe $\alpha_1, \alpha_2, \ldots \alpha_m$ von x durch p theilbar wird, muss dasselbe von $\varphi(x)$ gelten, d. h. die Congruenz

$$\varphi(x) \equiv 0 \pmod{p},$$

welche höchstens vom Grade $m - 1$ ist, hat mehr Wurzeln, als ihr Grad beträgt, was wegen der, bis zum Grade $m - 1$ vorausgesetzten Richtigkeit des Satzes nur geschehen kann, wenn sie identisch Statt findet. Die obige Gleichung lässt sich hiernach als Congruenz schreiben, wie folgt:

$$x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m \equiv (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_m) \pmod{p}.$$

Da nun die rechte Seite derselben für keinen mit $\alpha_1, \alpha_2, \ldots \alpha_m$ incongruenten Werth von x durch p theilbar sein kann, weil es keiner der Factoren wird und p Primzahl ist, so kann auch die Congruenz

$$x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m \equiv 0 \pmod{p}$$

keine Wurzeln weiter haben.

8. Betrachten wir als Beispiel die Congruenz:

$$(8) \qquad x^{p-1} - 1 \equiv 0 \pmod{p},$$

welche für die Folge von besonderer Wichtigkeit ist. Nach dem Fermat'schen Satze leistet derselben jede nicht durch p theilbare Zahl Genüge; die Congruenz (8) hat also genau soviel Wurzeln, als ihr Grad beträgt, nämlich die Wurzeln:

$$x \equiv 1, \; x \equiv 2, \; \ldots \; x \equiv p - 1 \pmod{p}.$$

Nach dem Ende der vorigen Nr. ergiebt sich daraus die Congruenz:

$$(9) \quad x^{p-1} - 1 \equiv (x - 1)(x - 2)\ldots(x - p + 1) \pmod{p};$$

sie wird uns weiterhin von grossem Nutzen sein. Vergleicht man die constanten Glieder auf den beiden Seiten derselben, so erhält man die folgende Congruenz:

$$(10) \qquad 1 . 2 . 3 \ldots (p - 1) \equiv -1 \pmod{p},$$

welche eine ausgezeichnete Eigenschaft der Primzahlen ausspricht und als Wilson'scher Satz bekannt ist.

9. Besondere Beachtung verdienen die Wurzeln der Congruenz (8), weil sie ähnliche Eigenschaften haben, wie die Einheitswurzeln, und darauf vor Allem die Auflösung der Kreistheilungsgleichung gegründet ist. In der That, ist m irgend eine Wurzel d. h. irgend eine, durch p nicht theilbare Zahl, so wird auch jede Potenz von m eine Wurzel sein, also die unendliche Reihe:

$$m, m^2, m^3, \ldots$$

lauter Wurzeln der Congruenz (8) enthalten. Unter denselben muss mindestens eine congruent Eins sein (mod. p), nämlich m^{p-1}, und wenn mit d der kleinste Exponent bezeichnet wird, für welchen $m^d \equiv 1$ (mod. p) ist, so zeigt sich, gerade wie in der vorigen Vorlesung, dass d ein Divisor von $p-1$ sein muss. Dann heisse m eine, zum Exponenten d gehörige Zahl. Man erkennt vermittelst derselben Betrachtungen, die wir dort angewendet haben, dass zu jedem Divisor d von $p-1$ als Exponent genau $\varphi(d)$ Wurzeln gehören. Nennt man insbesondere diejenigen Zahlen, welche zum Exponenten $p-1$ gehören, primitive Wurzeln (mod. p), so erhält man den wichtigen Satz: es giebt $\varphi(p-1)$ primitive Wurzeln (mod. p).

Ist g irgend eine derselben, so bilden die Potenzen

$$g, g^2, g^3, \cdots g^{p-1} \tag{11}$$

alle Wurzeln der Congruenz (8). Denn sie sind erstens sämmtlich offenbar Wurzeln derselben, sodann aber auch unter einander incongruent (mod. p); wäre nämlich $g^h \equiv g^k$ (mod. p), während h, k zwei Zahlen aus der Reihe $1, 2, 3, \ldots (p-1)$ bedeuten, von denen h die grössere sei, so könnte man beiderseitig mit g^k, welches nicht durch p theilbar ist, dividiren und fände $g^{h-k} \equiv 1$ (mod. p), was nicht angeht, da $h-k < p-1$ und g primitive Wurzel (mod. p) ist. Wir erhalten so das für das Folgende sehr bemerkenswerthe Resultat: dass die Zahlen der Reihe (11), wenn man von der Ordnung absieht, den Zahlen $1, 2, 3, \ldots p-1$ (mod. p) congruent sind; und da andererseits jede durch p nicht theilbare Zahl einer der letzteren Zahlen (mod. p) congruent sein muss, so wird jede durch p nicht theilbare Zahl auch einer bestimmten Zahl aus der Reihe (11) (mod. p) congruent sein.

10. Ist also m irgend eine durch p nicht theilbare Zahl, so giebt es eine Zahl μ aus der Reihe $1, 2, 3, \ldots p-1$, von der Art, dass

$$m \equiv g^\mu \pmod{p} \tag{12}$$

ist. Diese Zahl μ soll der Index von m heissen, in Zeichen: $\mu = \text{ind.}\, m$. Einige einfache Eigenschaften der Indices, welche in der Folge zur Anwendung kommen, sollen hier zusammengestellt werden.

1) Der Index eines Products ist der Summe der Indices der Faktoren mod. $(p-1)$ congruent. Denn, ist $\mu = \text{ind.}\, m$, $\nu = \text{ind.}\, n$, also $m \equiv g^{\mu}$, $n \equiv g^{\nu}$ (mod. p), so ist $mn \equiv g^{\mu+\nu}$ (mod. p); bezeichnet andererseits λ den ind. (mn), so ist $mn \equiv g^{\lambda}$, also ergiebt sich $g^{\lambda} \equiv g^{\mu+\nu}$ (mod. p). Nun sind λ, μ, ν drei Zahlen aus der Reihe $1, 2, 3, \ldots p-1$; ist daher $\mu + \nu < p - 1$, so muss, da die verschiedenen Potenzen der Reihe (11) als incongruent nachgewiesen sind, $\lambda = \mu + \nu$ sein, und dann ist auch $\lambda \equiv \mu + \nu$ mod. $(p-1)$. Wenn aber $\mu + \nu > p-1$ ist, so ist doch jedenfalls $\mu + \nu < 2(p-1)$, man kann also setzen $\mu + \nu = p - 1 + \varkappa$, während $\varkappa < p - 1$ ist; aus der Congruenz $g^{\lambda} \equiv g^{\mu+\nu}$ (mod. p) folgt dann, da $g^{p-1} \equiv 1$ ist, $g^{\lambda} \equiv g^{\varkappa}$, folglich $\varkappa = \lambda$, $\mu + \nu = p - 1 + \lambda$, also $\mu + \nu \equiv \lambda$ mod. $(p-1)$.

Nachdem auf diese Weise die Richtigkeit des Satzes für ein Product von zwei Factoren bewiesen worden, dehnt man ihn leicht auf ein Product von beliebig viel Factoren aus.

2) Ist der Modulus p gegeben, so ist gleichwohl der Index einer Zahl m noch nicht bestimmt, vielmehr hängt der Werth von ind. m offenbar ab von der willkürlichen Wahl der primitiven Wurzel g, auf welche man ihn bezieht. Wir haben nicht nöthig, auf diese Abhängigkeit hier weiter einzugehen, beschränken uns vielmehr auf die eine Bemerkung, dass zwei Zahlen, sowie die ihnen (mod. p) congruenten für alle primitive Wurzeln denselben Index beibehalten. Dies sind die Zahlen $+1$ und -1. Denn, welches auch die primitive Wurzel g sei, von den Potenzen (11) kann stets nur die letzte congruent Eins sein, es ist also stets:

$$\text{ind.}\,(1) = p - 1$$

$$\text{oder ind.}\,(1) \equiv 0 \text{ mod. } (p-1). \tag{13}$$

Ferner ist:

$$g^{p-1} - 1 = \left(g^{\frac{p-1}{2}} - 1\right)\left(g^{\frac{p-1}{2}} + 1\right) \equiv 0 \text{ (mod. } p),$$

also einer der beiden Factoren:

$$g^{\frac{p-1}{2}} - 1, \quad g^{\frac{p-1}{2}} + 1,$$

und zwar der letztere durch p theilbar, denn, wäre es der erste, so gehörte g nicht zum Exponenten $p-1$, was es als primitive Wurzel (mod. p) doch muss. Es folgt also:

(14) $\quad$ ind. (-1) oder ind. $(p-1) = \frac{p-1}{2}$.

3) Man beweist durch dieselben Betrachtungen, welche in Nr. 4 der vorigen Vorlesung angewendet worden sind, dass unter den Potenzen (11) diejenigen zum Exponenten d (mod. p) gehören, deren Exponenten mit $p-1$ den grössten gemeinsamen Divisor $\delta = \frac{p-1}{d}$ haben. Dies lässt sich auch als eine Eigenschaft der Indices folgendermassen aussprechen: Ist m eine zum Exponenten d (mod. p) gehörige Zahl und μ ihr Index, so ist der grösste gemeinsame Theiler der Zahlen μ und $p-1$ gleich $\frac{p-1}{d}$, und umgekehrt. In der That, ist $m \equiv g^{\mu}$, so gehört m nach dem eben Bemerkten nur dann zum Exponenten d, wenn μ und $p-1$ den grössten gemeinsamen Theiler $\frac{p-1}{d}$ besitzen.

Ist daher γ eine von g verschiedene primitive Wurzel, so ist ind. γ relative Primzahl zu $p-1$, und umgekehrt. Denn in diesem Falle hat d den Werth $p-1$, also $\frac{p-1}{d}$ den Werth Eins. —

Fünfte Vorlesung.

Von der Irreductibilität der Kreistheilungsgleichung.

1. Nächst den Eigenschaften der primitiven Wurzeln (mod. p) ist es, wie schon bemerkt, besonders die Irreductibilität der Kreistheilungsgleichung, auf welcher die Methode zu ihrer algebraischen Auflösung beruht. *) Eine ganze Function $f(x)$ mit rationalen Coëfficienten heisst aber irreductibel, wenn es nicht möglich ist, sie in Factoren mit ebenfalls rationalen Coëfficienten zu zerlegen. Ist $f(x)$ eine irreductible Function, so heisst die Gleichung $f(x)=0$ eine irreductible Gleichung.

---

*) Vergl. darüber Abel, mémoire sur une classe particulière d'équations résolubles algébriquement, in seinen oeuvres complètes pag. 114 oder in Crelle's J., Bd. 4, pag. 26.

Hier gilt nun folgender Hauptsatz:

Eine irreductible Gleichung $f(x) = 0$ *kann mit keiner Gleichung* $\varphi(x) = 0$ *von geringerem Grade und mit rationalen Coëfficienten eine Wurzel gemeinsam haben.* Denn sonst hätten die ganzen Functionen $f(x)$, $\varphi(x)$ einen, von $f(x)$ verschiedenen, grössten gemeinsamen Divisor, dessen Coëfficienten bekanntlich ebensowohl rational sein müssten, wie die der beiden Functionen, $f(x)$ hätte also gegen die vorausgesetzte Irreductibilität einen rationalen Factor.

Eine unmittelbare Folgerung aus diesem Satze ist der folgende:

Wenn eine irreductible Gleichung $f(x) = 0$ *eine Wurzel mit einer andern Gleichung* $F(x) = 0$ *gemeinsam hat, deren Coëfficienten rationale Zahlen sind, so genügen entweder alle ihre Wurzeln der Gleichung* $F(x) = 0$, *oder* $F(x)$ *ist identisch gleich Null.* Dies Letzte tritt nach dem vorigen Satze jedenfalls dann ein, wenn der Grad von $F(x)$ kleiner ist als der von $f(x)$. Im andern Falle kann man stets setzen:

$$F(x) = f(x) \,.\, Q(x) + \varphi(x),$$

worin $Q(x)$ der Quotient, $\varphi(x)$ der Rest ist, welchen die Division von $F(x)$ durch $f(x)$ ergiebt; Beides sind ganze Functionen mit rationalen Coëfficienten, die letzte von kleinerem Grade als $f(x)$. Haben nun $F(x)$, $f(x)$ eine gemeinsame Wurzel, d. h. finden für einen bestimmten Werth von x die Gleichungen $F(x) = 0$, $(x) = 0$ gleichzeitig statt, so muss dieser auch der Gleichung $\varphi(x) = 0$ genügen, woraus nach dem vorigen Satze folgt, dass $\varphi(x)$ identisch gleich Null, also

$$F(x) = f(x) \,.\, Q(x)$$

ist; dann genügen aber alle Wurzeln der Gleichung $f(x) = 0$ auch der Gleichung $F(x) = 0$.

Eine Gleichung $f(x) = 0$ mit ganzzahligen Coëfficienten, deren höchster gleich Eins, wird irreductibel sein, wenn es nicht möglich ist, $f(x)$ in Factoren mit ganzzahligen Coëfficienten zu zerlegen; denn nach Nr. 2 der vor. Vorl. findet dann auch eine Zerlegung in rationale Factoren nicht statt.

2. Die *Kreistheilungsgleichung*

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = 0,$$

d. i. *die Gleichung für die primitiven* p^{ten} *Einheits-*

wurzeln ist irreductibel. Dasselbe gilt von den allgemeineren Gleichungen, welche die primitiven Einheitswurzeln des Grades p^a oder eines beliebig zusammengesetzten Grades n zu Wurzeln haben. Von diesem Satze sind verschiedene Beweise gegeben worden, der erste, für einen Primzahlgrad geltende, von Gauss in den Disqu. arithm. art. 341; diesem folgten andere von Kronecker, Schoenemann, Eisenstein, Dedekind, Arndt u. A. Das gemeinsame Princip, welches allen diesen Beweisen, mehr oder weniger versteckt, zum Grunde liegt, besteht in Folgendem:

Bezeichnen wir mit $X = 0$ die fraglichen Gleichungen. Um zu beweisen, dass eine Zerlegung von X in Factoren $\varphi(x)$, $\psi(x)$ mit ganzzahligen Coëfficienten, d. i. die Gleichung

$$X = \varphi(x) \cdot \psi(x)$$

nicht möglich ist, genügt es offenbar zu zeigen, dass in Bezug auf irgend einen Modulus m die Congruenz

$$X \equiv \varphi(x) \cdot \psi(x) \pmod{m}$$

nicht stattfinden kann, denn diese würde in Bezug auf jeden Modulus eine unmittelbare Folgerung jener Gleichung sein.

Hierdurch fällt eigentlich die Frage nach der Irreductibilität der Gleichungen der Lehre von den höheren Congruenzen anheim, welche sich mit der Zerlegung der ganzen Functionen in Factoren in Beziehung auf einen gegebenen Modulus beschäftigt. Der Beweis von Schoenemann*), auf einen Primzahlgrad bezüglich, befindet sich denn auch in der That in einer Abhandlung über höhere Congruenzen und lässt das genannte Princip am Klarsten hervortreten. Auch Dedekind's Beweis**), welcher für den allgemeinsten Fall eines beliebig zusammengesetzten Grades gilt, knüpft unmittelbar an jene Lehre an. Hier sollen einige der angeführten Beweise mitgetheilt werden, welche sich ohne andere Hilfsmittel, als die in der vorigen Vorlesung gegebenen, auseinandersetzen lassen.

3. Die beiden Beweise von Kronecker***) und der-

*) Schoenemann, Theorie der höheren Congruenzen § 50.

**) Dedekind, Beweis für die Irreductibilität der Kreistheilungs-Gleichungen, Crelle's J., Bd. 54.

***) Kronecker, Beweis, dass für jede Primzahl p die Gleichung $x^{p-1} + \ldots + x + 1 = 0$ irreductibel ist, Crelle's J., Bd. 29 und Derselbe, démonstration de l'irréductibilité de l'équation $x^{n-1} + \ldots + x + 1 = 0$, où n désigne un nombre premier, Liouville's Journ., Bd. 1, 2. série.

jenige von Eisenstein*) beziehen sich zwar zunächst auf die Gleichung:

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = 0,$$

gestatten aber unmittelbar die Ausdehnung auf den Fall, wo der Grad der Einheitswurzeln die Potenz einer ungeraden Primzahl, gleich p^a ist**) und geben so den Beweis von der Irreductibilität der Gleichung

$$(1) \quad X = x^{p^{a-1}(p-1)} + x^{p^{a-1}(p-2)} + \ldots + x^{p^{a-1}} + 1 = 0.$$

Wir wollen also sogleich von dieser Gleichung handeln, welche jene als speciellen Fall in sich begreift.

Kronecker's Beweise sind einander sehr ähnlich. Nehmen wir an, X sei nicht irreductibel, sondern dem Producte zweier ganzer Functionen $\varphi(x)$, $\psi(x)$ mit ganzzahligen Coëfficienten gleich, in Zeichen:

$$X = \varphi(x) \cdot \psi(x),$$

so ergäbe sich, indem man $x = 1$ setzt:

$$p = \varphi(1) \cdot \psi(1),$$

einer der beiden, offenbar ganzzahligen Factoren, z. B. $\varphi(1)$, müsste daher gleich ± 1 sein. Da sich nun die Wurzeln der Gleichung (1) auf beide Factoren vertheilen, so sei ϱ eine derjenigen, welche der Gleichung $\varphi(x) = 0$ genügt. Welche primitive Wurzel der Gleichung $x^{p^a} = 1$ wir dann auch unter r verstehen mögen, die Reihe von Potenzen

$$(2) \qquad r, \; r^\alpha, \; r^\beta, \; \ldots \; r^\gamma,$$

in welcher $1, \alpha, \beta, \ldots \gamma$ sämmtliche, nicht durch p theilbare Zahlen der Reihe $1, 2, 3, \ldots p^a$ bezeichnen sollen, stellt (nach dem Zusatz in Nr. 4 der 3. Vorlesung) alle primitive Einheitswurzeln vom Grade p^a, d. i. alle Wurzeln der Gleichung (1) dar. Demnach befindet sich unter ihnen auch die Wurzel ϱ, und folglich ist

$$(3) \qquad \varphi(r) \cdot \varphi(r^\alpha) \cdot \varphi(r^\beta) \ldots \varphi(r^\gamma) = 0,$$

welche Wurzel der Gleichung (1) auch unter r verstanden werden mag. Der eine Kronecker'sche Beweis fährt nun fort:

---

*) Eisenstein, in Crelle's J., Bd. 39, pag. 167.

**) Serret, sur une question de théorie des nombres, Liouville's J., Bd. 15.

Da hiernach das Product:

$$\varphi(x) \, . \, \varphi(x^{\alpha}) \, . \, \varphi(x^{\beta}) \, . \, . \, . \, \varphi(x^{\gamma})$$

für jede Wurzel der Gleichung (1), welche als Einheitswurzeln desselben Grades nach Nr. 3 der 1. Vorlesung verschieden sind, verschwindet, so ist es einem elementaren algebraischen Satze zufolge durch X theilbar, d. h.

$$\varphi(x) \, . \, \varphi(x^{\alpha}) \, \varphi(x^{\beta}) \, . \, . \, . \, \varphi(x^{\gamma}) = X \, . \, F(x),$$

wo $F(x)$ eine ganze Function mit ganzzahligen Coëfficienten. Setzt man nun $x = 1$, so ergiebt sich, da die Anzahl der Factoren gleich der Anzahl der Zahlen $1, \alpha, \beta, \ldots \gamma$, also gleich $p^{a-1}(p-1)$ ist,

$$\varphi(1)^{p^{a-1}(p-1)} = p \, . \, F(1);$$

$\varphi(1)^{p^{a-1}(p-1)}$, welches den Werth Eins hat, wäre also durch p theilbar, was nicht sein kann. Daher ist die Gleichung (1) irreductibel.

4. Von diesem Beweise unterscheidet sich der andere Kronecker'sche nur dadurch, dass dort direct die Richtigkeit der Congruenz:

$$\varphi(r) \, . \, \varphi(r^{\alpha}) \, . \, \varphi(r^{\beta}) \, . \, . \, . \, \varphi(r^{\gamma}) \equiv \varphi(1)^{p^{a-1}(p-1)} \pmod{p}$$

gezeigt wird, welche wieder, wenn $\varphi(1) = \pm 1$ ist, nach Gleichung (3) auf einen Widerspruch führt. Jener Nachweis lässt sich folgendermassen geben:

Wenn $\varphi(r)$, wie es hier stattfindet, eine ganze und ganzzahlige Function der Wurzel r von (1) ist, so ist einerseits

$$\varphi(r) \, . \, \varphi(r^{\alpha}) \, . \, \varphi(r^{\beta}) \, . \, . \, . \, \varphi(r^{\gamma})$$

als symmetrische Function aller Wurzeln dieser Gleichung bekanntlich eine ganze und ganzzahlige Function ihrer Coëfficienten, also, da diese selbst ganze Zahlen sind, eine ganze Zahl, welche wir mit A bezeichnen wollen, also:

$$\varphi(r) \, . \, \varphi(r^{\alpha}) \, . \, \varphi(r^{\beta}) \, . \, . \, . \, \varphi(r^{\gamma}) = A.$$

Andererseits ist nach der Formel (6) der vorigen Vorlesung für jedes x:

$$\varphi(x)^p = \varphi(x^p) + p \, . \, f(x),$$

wo $f(x)$ eine ganze und ganzzahlige Function von x ist. Bildet man nach dieser Gleichung das Product:

$$A^p = \varphi(r)^p \, . \, \varphi(r^{\alpha})^p \, . \, . \, . \, \varphi(r^{\gamma})^p,$$

so erhält man zunächst das Glied:

$$\varphi(r^p) \,.\, \varphi(r^{\alpha p}) \ldots \varphi(r^{\gamma p}),$$

und dann einen durch p theilbaren Ausdruck, welcher offenbar symmetrisch in Bezug auf alle Wurzeln $r, r^\alpha, r^\beta, \ldots r^\gamma$ der Gleichung (1), folglich eine durch p theilbare ganze Zahl ist. Dies ergiebt die Congruenz

$$A^p \equiv \varphi(r^p) \,.\, \varphi(r^{\alpha p}) \ldots \varphi(r^{\gamma p}) \quad (\text{mod. } p),$$

oder nach dem Fermat'schen Satze:

$$A \equiv \varphi(r^p) \,.\, \varphi(r^{\alpha p}) \ldots \varphi(r^{\gamma p}) \quad (\text{mod. } p).$$

Durch wiederholte Erhebung zur p^{ten} Potenz folgt allgemeiner für jedes positive ganze m:

$$A \equiv \varphi(r^{p^m}) \,.\, \varphi(r^{\alpha p^m}) \ldots \varphi(r^{\gamma p^m}) \quad (\text{mod. } p);$$

setzt man daher $m = a$, wofür $r^{p^a} = 1$ wird, so ergiebt sich, wie behauptet wurde: A oder

$$\varphi(r)\,\varphi(r^\alpha)\,\varphi(r^\beta) \ldots \varphi(r^\gamma) \equiv \varphi(1)^{p^{a-1}(p-1)} \quad (\text{mod. } p).$$

5. Während diese Beweise sich wesentlich auf die Natur der Einheitswurzeln stützen, ist Eisenstein's Beweis davon unabhängig, beruht dagegen auf der Beschaffenheit der Coëfficienten der fraglichen Gleichungen. Das Princip dieses Beweises ist der folgende Satz:

Eine Gleichung $f(x) = 0$ ist irreductibel, sobald der höchste Coëfficient in $f(x)$ gleich Eins, der letzte gleich $\pm p$, die mittleren durch p theilbar sind. Denn, wäre im Gegentheil $f(x)$, dessen Grad $m + n$ sei, in ganzzahlige Factoren zerlegbar, sodass

$$f(x) = (x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m)$$
$$(x^n + b_1 x^{n-1} + \ldots + b_{n-1} x + b_n),$$

so müssten beide Ausdrücke auch (mod. p) congruent sein. Die Vergleichung der constanten Glieder auf beiden Seiten liefert zunächst

$$\pm p = a_m \,.\, b_n,$$

also etwa $a_m = \pm 1$, $b_n = \pm p$. Lässt man aber in der Congruenz:

$$f(x) \equiv (x^m + a_1 x^{m-1} + \ldots + a_{m-1} x \pm 1)$$
$$(x^n + b_1 x^{n-1} + \ldots + b_{n-1} x \pm p) \quad (\text{mod. } p)$$

alle durch p theilbare Glieder fort, so erhält man:

$$x^{m+n} \equiv (x^m + a_1 x^{m-1} + \ldots \pm 1)$$
$$(x^n + b_1 x^{n-1} + \ldots + b_{n-1} x) \quad (\text{mod. } p).$$

Rechts findet sich nun das Glied $\pm b_{n-1} x$, welchem links kein Glied entspricht, also muss b_{n-1} durch p theilbar sein, und indem man es weglässt, ergiebt sich:

$$x^{m+n} \equiv (x^m + a_1 x^{m-1} + \ldots \pm 1)$$
$$(x^n + b_1 x^{n-1} + \ldots + b_{n-2} x^2) \quad (\text{mod. } p),$$

woraus in ähnlicher Weise folgt, dass b_{n-2} durch p theilbar ist. So fortfahrend gelangt man endlich zu der Congruenz:

$$x^{m+n} \equiv (x^m + a_1 x^{m-1} + \ldots \pm 1)\, x^n \quad (\text{mod. } p),$$

welche unmöglich ist, da der Coëfficient von x^n rechts $\equiv \pm 1$ (mod. p), links aber gleich Null ist. Hieraus geht die Unzulässigkeit der Annahme, also die Wahrheit des Satzes hervor.

Wenn man nun in der Gleichung (1) die Substitution $x = z + 1$ macht, so wird

$$(4) \qquad X = F(z)$$

werden, wo $F(z)$ eine ganze Function von z von demselben Grade wie X und mit ganzzahligen Coëfficienten ist, deren höchster offenbar gleich Eins ist. Für $z = 0$ reducirt sich $F(z)$ auf den letzten Coëfficienten, dessen Werth sich gleich p, nämlich gleich dem Werthe von X für $x = 1$ ergiebt. Beachtet man ferner, dass

$$x^p \equiv z^p + 1,\ x^{p^2} \equiv z^{p^2} + 1, \ldots x^{p^{a-1}} \equiv z^{p^{a-1}} + 1,$$
$$x^{p^a} \equiv z^{p^a} + 1 \quad (\text{mod. } p)$$

ist, so führt die Gleichung (4), welche auch so geschrieben werden kann:

$$F(z) \,.\, (x^{p^{a-1}} - 1) = x^{p^a} - 1,$$

auf die Congruenz:

$$F(z) \equiv z^{p^{a-1}(p-1)} \quad (\text{mod. } p),$$

und lehrt, dass auch die mittleren Coëfficienten von $F(z)$ durch p theilbar sind. Da somit die Gleichung $F(z) = 0$ sich in dem Falle des vorigen Satzes befindet, ist sie irreductibel; daraus folgt aber nach der Gleichung (4) offenbar auch die Irreductibilität der Gleichung $X = 0$.

6. Unter den Beweisen für die Irreductibilität der allgemeinen Gleichung, deren Wurzeln die primitiven

Einheitswurzeln eines beliebig zusammengesetzten Grades n sind, wähle ich denjenigen von Arndt*) als besonders einfach aus.

Arndt bedient sich seines Princips zunächst zum Beweise von der Irreductibilität der Gleichung (1). Der Kürze wegen nehmen wir diese nach dem Vorigen als bekannt an, setzen sogar voraus, die Irreductibilität für die Gleichung

$$F_n(x) = 0,$$

deren Wurzeln die primitiven n^{ten} Einheitswurzeln sind, sei bereits bewiesen für jedes n, welches aus nicht mehr als k verschiedenen Primfactoren besteht; lässt sich dann die Irreductibilität auch für solche n beweisen, welche einen Primfactor mehr enthalten, so steht sie offenbar fest für jedes mögliche n. Dieser Nachweis aber kann, wie folgt, gegeben werden:

Wir setzen $n = p^a \,.\, n'$, wo n' aus k, von p verschiedenen Primzahlen besteht. Angenommen nun, es sei

$$F_n(x) = \varphi(x) \,.\, \psi(x)$$

und

$$\Phi(x) = 0, \quad \Psi(x) = 0$$

seien die Gleichungen, welche die $p^{a\,ten}$ Potenzen der Wurzeln von

$$\varphi(x) = 0, \quad \psi(x) = 0$$

resp. zu Wurzeln haben, so wird durch a-Mal wiederholte Anwendung des Satzes, welcher Nr. 6 der vorigen Vorlesung beschliesst,

$$(5) \qquad \varphi(x) \equiv \Phi(x), \quad \psi(x) \equiv \Psi(x) \quad (\text{mod. } p)$$

erhalten werden.

Jede primitive n^{te} Einheitswurzel r kann nun, wie sich aus Nr. 6 der 3. Vorlesung sehr leicht ergiebt, gleich dem Producte aus einer primitiven Einheitswurzel ϱ vom Grade p^a und einer andern ω vom Grade n' gesetzt werden; aus der Gleichung $r = \varrho \,.\, \omega$ folgt aber durch Erhebung zur Potenz p^a die Gleichung $r^{p^a} = \omega^{p^a}$ d. h., da p^a zu n' prim ist, r^{p^a} gleich einer pri-

*) Arndt, einfacher Beweis für die Irreductibilität einer Gleichung in der Kreistheilung, in Crelle's J., Bd. 56. Eine Modification dieses Beweises ist derjenige von Lebesgue, s. in Liouville's J., Bd. 4, 2. série, démonstration de l'irréductibilité de l'équation aux racines primitives de l'unité.

mitiven Einheitswurzel ω' vom Grade n' (vgl. Zusatz zu Nr. 4 der 3. Vorlesung). Lässt man nun r successive je eine Wurzel der Gleichung $\varphi(x) = 0$ und der Gleichung $\psi(x) = 0$ bedeuten, so wird dem entsprechend r^{p^a} eine Wurzel der Gleichung $\Phi(x)=0$ oder $\Psi(x)=0$ sein, und daher wird jede dieser letztern Gleichungen irgend eine Wurzel mit der Gleichung

$$(6) \qquad F_{n'}(x) = 0$$

gemeinsam haben, folglich, da diese nach der Voraussetzung irreductibel ist, durch alle Wurzeln derselben befriedigt werden.

Ist demnach ω irgend eine Wurzel von (6), so folgt aus den Congruenzen (5):

$$\varphi(\omega) \equiv 0, \quad \psi(\omega) \equiv 0 \quad (\text{mod. } p),$$

mithin

$$(7) \qquad F_n(\omega) = p^2 \,.\, f(\omega),$$

wenn $f(\omega)$ eine gewisse ganze und ganzzahlige Function von ω bedeutet.

Bemerkt man andererseits die Gleichungen:

$$x^n - 1 = \prod_{d:n} F_d(x), \quad x^{\frac{n}{p}} - 1 = \prod_{\delta:\frac{n}{p}} F_\delta(x),$$

in welchen (vgl. 3. Vorlesung Nr. 5) der Index d alle Divisoren von n, der Index δ alle Divisoren von $\frac{n}{p}$ zu durchlaufen hat, und beachtet, dass letztere sich sämmtlich unter den erstern befinden, dass aber der Werth $d = n$ unter den Divisoren δ sich nicht findet, so zeigt sich, dass der Quotient $\frac{x^n - 1}{x^{\frac{n}{p}} - 1}$ eine durch $F_n(x)$ theilbare ganze Function, also

$$\frac{x^n - 1}{x^{\frac{n}{p}} - 1} = F_n(x) \,.\, F(x)$$

ist, worin $F(x)$ eine ganze und ganzzahlige Function. Setzt man hierin $x = \omega$, so ergiebt sich:

$$p = F_n(\omega) \,.\, F(\omega),$$

woraus in Verbindung mit der Gleichung (7) die folgende erhalten wird:

$$1 = p \,.\, f(\omega) \,.\, F(\omega).$$

Aus dem entwickelten Producte $f(\omega) . F(\omega)$ kann man aber mittels der identischen Gleichung $F_{n'}(\omega) = 0$ vom Grade $\varphi(n')$ alle höheren Potenzen von ω als die Potenz $\omega^{\varphi(n')-1}$ fortschaffen und findet so eine Gleichung von der Form:

$$1 = p\,(a_0 + a_1\,\omega + \ldots + a_{\varphi(n')-1} \,.\, \omega^{\varphi(n')-1}),$$

welche wegen der vorausgesetzten Irreductibilität der Gleichung (6) identisch bestehen muss und dann zu der unmöglichen Gleichung führt:

$$1 = p\,a_0.$$

Hieraus folgt die Irreductibilität der Gleichung

$$F_n(x) = 0.$$

7. Ein anderer Beweis, durch welchen die Irreductibilität dieser Gleichung sogar in einem weiteren Sinne, als wir dem Worte beigelegt haben, dargethan wird, rührt von Kronecker her.*) Es würde zu weit führen, denselben hier vollständig wiederzugeben; während wir daher den Leser auf Kronecker's Abhandlung selber verweisen müssen, entnehmen wir gleichwohl derselben die Principien zum Beweise eines Satzes, der zur Begründung einer späteren Behauptung benutzt werden soll. Wir sprechen folgenden Satz aus, in welchem $p - 1 = e \,.\, f$ gesetzt sein soll:

Die Function

$$X = x^{p-1} + x^{p-2} + \ldots + x + 1$$

kann nicht in Factoren zerlegt werden, deren Coëfficienten rationale und ganzzahlige Functionen einer Wurzel der irreductibeln Gleichung

$$F_e(x) = 0 \tag{8}$$

sind.

Zunächst bemerken wir, dass, wenn α eine Wurzel dieser Gleichung bedeutet, jede rationale Function von α auf die Form:

$$\frac{a_0 + a_1\,\alpha + \ldots + a_{\varepsilon-1} \,.\, \alpha^{\varepsilon-1}}{m} \tag{9}$$

gebracht werden kann, in welcher $a_0, a_1, \ldots a_{\varepsilon-1}$ und m ganze Zahlen sind, deren letzte nicht mit allen Coëfficienten a denselben gemeinsamen Factor hat, und worin ε zur Abkürzung für $\varphi(e)$

*) Kronecker, mémoire sur les facteurs irréductibles de l'équation $x^n = 1$, in Liouville's J., Bd. 19.

gesetzt ist. In der That, die rationale Function $\frac{f(\alpha)}{\varphi(\alpha)}$, unter $f(\alpha)$, $\varphi(\alpha)$ zwei ganze und ganzzahlige Functionen von α verstanden, kann, wenn $\alpha', \alpha'', \ldots \alpha^{(\varepsilon-1)}$ die übrigen Wurzeln der Gleichung (8) sind, auch so geschrieben werden:

$$\frac{f(\alpha) \cdot \varphi(\alpha') \, \varphi(\alpha'') \ldots \varphi(\alpha^{(\varepsilon-1)})}{\varphi(\alpha) \cdot \varphi(\alpha') \, \varphi(\alpha'') \ldots \varphi(\alpha^{(\varepsilon-1)})}.$$

Hierin ist aber der Nenner als symmetrische Function aller primitiven e^{ten} Einheitswurzeln eine ganze und ganzzahlige Function von den Coëfficienten der Gleichung (8), folglich einer ganzen Zahl m gleich. Im Zähler aber ist bekanntlich das Product $\varphi(\alpha') \, \varphi(\alpha'') \ldots \varphi(\alpha^{(\varepsilon-1)})$ und also auch der ganze Zähler einer ganzen Funktion von α mit ganzen Coëfficienten gleich, deren Grad vermittelst der identischen Gleichung

$$F_e(\alpha) = 0 \tag{10}$$

vom Grade ε kleiner als ε gemacht, und welche demnach auf die Form:

$$a_0 + a_1 \alpha + \ldots + a_{\varepsilon-1} \alpha^{\varepsilon-1}$$

reducirt werden kann. Da endlich jeder Factor, welchen m etwa mit allen Zahlen $a_0, a_1, \ldots a_{\varepsilon-1}$ gemeinsam haben sollte, weggehoben werden kann, erhält die rationale Function von α die in (9) behauptete Gestalt.

Nehmen wir nun an, X sei in die Factoren $\varphi(x)$, $\psi(x)$ zerlegbar, deren Coëfficienten rational von α abhangen, so ergiebt sich aus der Gleichung

$$X = \varphi(x) \cdot \psi(x),$$

wenn $x = 1$ gesetzt wird:

$$p = \varphi(1) \cdot \psi(1), \tag{11}$$

worin offenbar $\varphi(1)$, $\psi(1)$ rationale und ganzzahlige Functionen von α sein werden, sodass nach dem eben Bemerkten

$$\varphi(1) = \frac{a_0 + a_1 \alpha + \ldots + a_{\varepsilon-1} \alpha^{\varepsilon-1}}{m} = \frac{A(\alpha)}{m},$$

$$\psi(1) = \frac{b_0 + b_1 \alpha + \ldots + b_{\varepsilon-1} \alpha^{\varepsilon-1}}{n} = \frac{B(\alpha)}{n}$$

gesetzt und m ohne gemeinsamen Theiler mit allen a, n ohne gemeinsamen Theiler mit allen b angenommen werden kann. Hierdurch geht die Gleichung (11) in die folgende über:

$$p \cdot mn = A(\alpha) \cdot B(\alpha).$$

Diese lehrt, dass nur in einer der beiden Functionen $A(\alpha)$, $B(\alpha)$ alle Coëfficienten durch p theilbar sein können; denn wäre im Gegentheil gleichzeitig

$$(12) \qquad A(\alpha) = p \, . \, C(\alpha), \quad B(\alpha) = p \, . \, D(\alpha),$$

während $C(\alpha)$, $D(\alpha)$ ganze Functionen von α mit ganzen Coëfficienten sind, so folgte einerseits, dass weder m noch n durch p theilbar sind, andererseits die Gleichung:

$$mn = p \, . \, C(\alpha) \, D(\alpha),$$

welche vermittelst der Gleichung (10) auf die Form

$$mn = p(c_0 + c_1 \alpha + \ldots + c_{e-1} \, . \, \alpha^{e-1})$$

gebracht werden könnte und wegen der Irreductibilität der Gleichung (8) zu der Folgerung $mn = pc_0$ führen würde, die unzulässig ist, da keine der Zahlen m, n durch p theilbar ist.

Nun ist aber im Gegentheil leicht zu zeigen, dass die Gleichungen (12) aus der angenommenen Zerlegung von X mit Nothwendigkeit folgen. Denn, da $\varphi(x)$ jedenfalls eine Wurzel der Kreistheilungsgleichung enthält, so besteht $\varphi(1)$ aus einem oder mehreren Factoren von der Form $1 - r^h$, und diese liefern, da $r^p = 1$ ist, zur p^{ten} Potenz erhoben einen in r ganzen und ganzzahligen Ausdruck, dessen sämmtliche Coëfficienten durch p theilbar sind; daher ist auch

$$\varphi(1)^p = p \, . \, f(r)$$

also

$$(13) \qquad A(\alpha)^p = p \, . \, m^p \, . \, f(r)$$

wo $f(r)$ eine ganze und ganzzahlige Function von r bezeichnet. Bemerkt man hierauf, dass in der Entwicklung des Products

$$[z - pm^p f(r)] \, [z - pm^p f(r^2)] \ldots [z - pm^p \, . \, f(r^p)]$$

nach Potenzen von z das höchste Glied gleich z^p, die Coëfficienten aller andern Glieder aber als symmetrische Functionen aller p^{ten} Einheitswurzeln ganze Zahlen sind, welche offenbar den Factor p haben, so kann man jenes Product gleich

$$z^p - p \, . \, F(z)$$

setzen, wo $F(z)$ eine ganze und ganzzahlige Function von z ist, und erhält, da es für $z = A(\alpha)^p$ wegen Gleichung (13) verschwindet,

$$(14) \qquad A(\alpha)^{p^2} = p \, . \, \Phi(\alpha),$$

wo $\Phi(\alpha)$ eine ganze Function von α mit ganzen Coëfficienten ist,

wie sie offenbar durch die Substitution von $A(\alpha)^p$ an Stelle von z aus $F(z)$ entsteht. Da aber $p = ef + 1$, also $\alpha^p = \alpha$ ist, und nach Gleichung (7) der 4. Vorlesung

$$A(\alpha)^p \equiv A(\alpha^p) \pmod{p}$$

gesetzt werden kann, so ergiebt sich:

$$A(\alpha)^p \equiv A(\alpha)$$

also auch weiter:

$$A(\alpha)^{p^2} \equiv A(\alpha) \pmod{p}$$

oder $A(\alpha)^{p^2} = A(\alpha) + p\Phi'(\alpha)$, wenn auch $\Phi'(\alpha)$ eine Function mit ganzzahligen Coëfficienten. Die Gleichung (14) liefert demnach ein Resultat, wie die erste der Gleichungen (12):

$$A(\alpha) = p \,.\, C(\alpha).$$

Nichts hindert aber, auf demselben Wege sich zu überzeugen, dass auch

$$B(\alpha) = p \,.\, D(\alpha)$$

ist, wie behauptet wurde.

Da somit durch die Annahme der Zerlegbarkeit der Function X ein Widerspruch entsteht, so erhellt ihre Unzerlegbarkeit.

Nachdem auf diese Weise die Irreductibilität der Kreistheilungsgleichung in einem weiteren Sinne wie früher dargethan worden ist, werden die Folgerungen, welche in Nr. 1 aus dem Begriffe der irreductibeln Gleichungen geschlossen worden sind, jetzt in derselben weiteren Bedeutung bestehen bleiben.

Sechste Vorlesung.

Die Gaussische Methode zur Auflösung der Kreistheilungsgleichung. Die Perioden und ihre Eigenschaften.

1. Wir haben im Vorigen die Aufgabe, den Kreis in p gleiche Theile zu theilen, wenn p eine ungerade Primzahl bedeutet, auf die Auflösung der Gleichung

$$(1) \qquad X = x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$$

zurückgeführt. Indem nach den vorbereitenden Betrachtungen der letzten Vorlesungen nunmehr die Gaussische Methode mitgetheilt

werden soll, durch welche die algebraische Auflösbarkeit dieser Gleichung dargethan wird, müssen wir mit Hilfe der primitiven Wurzeln (mod. p) unter ihren Wurzeln eine eigenthümliche Ordnung herstellen, auf welcher, wie sich zeigen wird, jene Methode wesentlich begründet ist.

Die Wurzeln der Gleichung (1) waren die Potenzen:

$$(2) \qquad r,\ r^2,\ r^3,\ \ldots\ r^{p-1}$$

wenn r irgend eine Wurzel bezeichnet. Nun haben wir einerseits gesehen, dass $r^h = r^{h'}$ ist, sobald $h \equiv h'$ (mod. p); andererseits waren nach Nr. 9 der vierten Vorlesung die Potenzen:

$$(3) \qquad 1,\ g,\ g^2,\ \ldots\ g^{p-2}$$

einer primitiven Wurzel g von p den Zahlen $1,\ 2,\ 3,\ \ldots\ p-1$, wenn auch in anderer Ordnung, (mod. p) congruent. Daraus ergiebt sich offenbar, dass die Potenzen (2), von der Reihenfolge abgesehen, mit den folgenden Potenzen:

$$(4) \qquad r,\ r^g,\ r^{g^2},\ \ldots\ r^{g^{p-2}}$$

übereinstimmen müssen. Die Wurzeln der Gleichung (1) werden also auch durch diese Reihe gegeben, deren einzelne Glieder die bemerkenswerthe Eigenschaft haben, dass jedes die g^{te} Potenz des vorhergehenden ist; dies gilt auch vom ersten Gliede r, welches nach der Congruenz $g^{p-1} \equiv 1$ (mod. p) gleich $r^{g^{p-1}}$ gesetzt, d. i. als g^{te} Potenz des letzten angesehen werden kann. Die Wurzeln der Gleichung (1) können also, allgemeiner ausgedrückt, so geordnet werden, dass jede dieselbe rationale Function der vorhergehenden ist, wie die erste von der letzten.

2. Schalten wir noch eine allgemeine Bemerkung hier ein. Die Methoden zur algebraischen Auflösung von Gleichungen beruhen im Grunde auf dem Princip, dass man gewisse ganze Functionen von den Wurzeln der Gleichung bildet, deren Bestimmung von einer anderen Gleichung geringeren Grades oder leichterer Behandlung abhängig ist, und welche so beschaffen sind, dass, wenn man ihre Werthe gefunden hat, man daraus auch leicht die Werthe der Wurzeln der gegebenen Gleichung selber ermitteln kann. Dieser Umstand kann schon bei der einfachsten Gleichung, der allgemeinen quadratischen Gleichung

$$x^2 - ax + b = 0$$

bemerkt werden. Sind x_1, x_2 die beiden Wurzeln derselben, so sind die beiden Functionen von denselben:

$$x_1 + x_2, \quad x_1 x_2$$

unmittelbar bekannt, nämlich $x_1 + x_2 = a$, $x_1 x_2 = b$. Daraus findet man:

$$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4 x_1 x_2 = a^2 - 4b,$$

also ist die Wurzelfunction

$$x_1 - x_2 = \pm \sqrt{a^2 - 4b},$$

und die Verbindung dieser und der andern Gleichung $x_1 + x_2 = a$ liefert sofort die beiden Wurzeln:

$$x_1 = \frac{a \pm \sqrt{a^2 - 4b}}{2}, \quad x_2 = \frac{a \mp \sqrt{a^2 - 4b}}{2}.$$

3. Betrachten wir nach dieser Bemerkung zunächst irgend eine ganze Function von den Wurzeln der Kreistheilungsgleichung:

$$F(r, r^2, r^3, \ldots r^{p-1});$$

diese kann offenbar auch als eine ganze Function der einen beliebigen Wurzel r aufgefasst werden und soll dann mit $f(r)$ bezeichnet werden. Man kann sie stets auf die Form:

$$f(r) = a_0 + a_1 r + a_2 r^2 + \ldots + a_m r^m$$

bringen oder, indem man jeden Exponenten von r, welcher $> p$ ist, durch seinen kleinsten Rest (mod. p) ersetzt, auf die andere Form:

$$f(r) = b_0 + b_1 r + b_2 r^2 + \ldots + b_{p-1} \cdot r^{p-1},$$

und darin werden die Coëfficienten nothwendig ganze und ganzzahlige Functionen von den in F enthaltenen Coëfficienten sein, sodass sie z. B. rationale oder ganze Zahlen sein werden, jenachdem es die Coëfficienten in F sind. Zieht man von der letzten Gleichung die Gleichung (1) ab, nachdem man sie mit b_0 multiplicirt und $x = r$ gesetzt hat, so erhält man endlich die Function unter folgender Form:

$$(5) \qquad A_1 r + A_2 r^2 + \ldots + A_{p-1} \cdot r^{p-1}.$$

Diese soll als ihre Normalform bezeichnet werden, weil $f(r)$ in dieselbe nur auf eine ganz bestimmte Weise gebracht werden kann, sobald die Coëfficienten in F rationale Zahlen, oder allgemeiner rationale und ganzzahlige Functionen irgend einer Wurzel α der Gleichung $x^{p-1} = 1$ sind, die beiden einzigen Fälle, welche

uns in der Folge interessiren werden. Fände man sie dann nämlich auch noch gleich

$$(5^a) \qquad B_1 r + B_2 r^2 + \ldots + B_{p-1} \cdot r^{p-1},$$

so müssten die beiden Ausdrücke (5) und (5^a) auch unter einander gleich sein, woraus durch Division mit r die Gleichung

$$A_1 - B_1 + (A_2 - B_2)\, r + \ldots + (A_{p-1} - B_{p-1})\, r^{p-2} = 0$$

vom Grade $p - 2$ sich ergäbe; wegen der Irreductibilität der Gleichung (1) in dem weiteren Sinne der Nr. 7 voriger Vorlesung müssten also die einzelnen Coëfficienten dieser Gleichung, welche, je nach jenen beiden Fällen, rationale Zahlen oder rationale Functionen von α sein werden, verschwinden, und dann würden die beiden Ausdrücke für die Function $f(r)$ vollständig identisch sein.

In der Normalform (5) kann man statt der Exponenten $1, 2, 3, \ldots p-1$ wieder die, ihnen (mod. p) congruenten Potenzen von g setzen, und, wenn man sodann nach den steigenden Potenzen von g ordnet, erhält man statt des Ausdruckes (5) den folgenden:

$$(6) \qquad f(r) = a_0 r + a_1 r^g + a_2 r^{g^2} + \ldots + a_{p-2} \cdot r^{g^{p-2}},$$

in welchem der Zusammenhang der Coëfficienten a mit den A leicht anzugeben ist. Ist nämlich $h \equiv g^k$, so ist $k = \text{ind. } h$; da nun der Potenz $r^h = r^{g^k}$ einerseits der Coëfficient A_h, andererseits der Coëfficient a_k entspricht, so hat man allgemein

$$A_h = a_k = a_{\text{ind. } h}.$$

Als Resultat dieser ganzen Untersuchung sprechen wir den Satz aus: Jede ganze Function von den Wurzeln der Kreistheilungsgleichung kann als ganze Function einer Wurzel jener Gleichung auf die Normalform (6) gebracht werden, in welcher die Coëfficienten ganze und ganzzahlige Functionen von den Coëfficienten der gegebenen Function sind.

4. Eine besondere Gattung solcher ganzer Functionen spielt nun bei der Gaussischen Auflösung der Gleichung (1) eine grosse Rolle. Denken wir uns die Zahl $p - 1$ irgendwie in zwei Factoren zerlegt, $p - 1 = e \cdot f$, und vertheilen die Grössen (4) in folgende e Gruppen von f Gliedern:

$$\begin{array}{l} r, \; r^{g^e}, \; r^{g^{2e}}, \; \ldots \; r^{g^{(f-1)e}} \\ r^g, \; r^{g^{e+1}}, \; r^{g^{2e+1}}, \; \ldots \; r^{g^{(f-1)e+1}} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ r^{g^{e-1}}, \; r^{g^{2e-1}}, \; r^{g^{3e-1}}, \; \ldots \; r^{g^{fe-1}}, \end{array}$$

wo die, jeder einzelnen Gruppe angehörigen Wurzeln wieder die Eigenschaft haben, dass jede derselben dieselbe rationale Function der vorhergehenden, wie die erste von der letzten, nämlich die $g^{e\,te}$ Potenz derselben ist, so sollen die Summen:

$$\begin{array}{l} \eta_0 = r + r^{g^e} + r^{g^{2e}} + \ldots + r^{g^{(f-1)e}} \\ \eta_1 = r^g + r^{g^{e+1}} + r^{g^{2e+1}} + \ldots + r^{g^{(f-1)e+1}} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \eta_{e-1} = r^{g^{e-1}} + r^{g^{2e-1}} + r^{g^{3e-1}} + \ldots + r^{g^{fe-1}} \end{array}$$

als besonders wichtig mit einem besonderen Namen bezeichnet und (f-gliedrige) Perioden genannt werden.

Diese haben zunächst die Eigenschaft, unverändert zu bleiben, wenn man in ihnen die Wurzel r durch irgend eine andere Wurzel der Periode η_0 ersetzt, dagegen sich cyclisch zu vertauschen, wenn r durch eine Wurzel ersetzt wird, welche einer der andern Perioden angehört. Wird nämlich r durch r^{g^e} ersetzt, so geht für jedes k

$$r^{g^k} + r^{g^{e+k}} + \ldots + r^{g^{(f-2)e+k}} + r^{g^{(f-1)e+k}}$$

über in:

$$r^{g^{e+k}} + r^{g^{2e+k}} + \ldots + r^{g^{(f-1)e+k}} + r^{g^k}$$

d. i. η_k bleibt bei der Substitution von r^{g^e} statt r, allgemeiner also von $r^{g^{me}}$ statt r ungeändert. Hiernach kann man die Indices der Perioden η auch über $e - 1$ wachsen lassen, indem dann jedesmal $\eta_{k'} = \eta_k$ ist, sobald $k' \equiv k \pmod{e}$.

Wird nun allgemeiner r durch r^{g^h} ersetzt, so gehen die Perioden $\eta_0, \eta_1, \eta_2, \ldots \eta_{e-1}$ über in $\eta_h, \eta_{h+1}, \ldots \eta_{h+e-1}$ oder in $\eta_h, \eta_{h+1}, \ldots \eta_{e-1}, \eta_0, \eta_1, \ldots \eta_{h-1}$ d. h. sie werden nur um h Stellen, wie man sich ausdrückt, cyclisch verschoben.

Die Vertheilung aller Wurzeln der Gleichung (1) in Perioden ist von der Wahl der primitiven Wurzel g unabhängig. Denn, sei γ eine von g verschiedene primitive

Wurzel (mod. p) und $\gamma \equiv g^h$ (mod. p), so ist nach dem Schlusssatze der 4. Vorlesung h zu $p-1$, also zu jedem der Factoren e, f relative Primzahl. Bezeichnet man die neuen Perioden mit $\varepsilon_0, \varepsilon_1, \varepsilon_2, \ldots \varepsilon_{e-1}$, so ist

$$\varepsilon_0 = r + r^{g^{he}} + r^{g^{2he}} + \ldots + r^{g^{(f-1)he}}.$$

Da aber die Zahlen 0, h, $2h$, ... $(f-1)h$ den Zahlen 0, 1, 2, ... $f-1$, wenn auch in anderer Ordnung, (mod. f) congruent sind, so sind 0, he, $2he$, ... $(f-1)he$, von der Reihenfolge abgesehen, den Zahlen 0, e, $2e$, ... $(f-1)e$ mod. $(p-1)$ congruent, und folglich $\varepsilon_0 = \eta_0$. Ebenso findet man:

$$\varepsilon_1 = \eta_h, \quad \varepsilon_2 = \eta_{2h}, \ldots \varepsilon_{e-1} = \eta_{(e-1)h}.$$

Nun sind wieder die Zahlen 0, h, $2h$, ... $(e-1)h$ den Zahlen 0, 1, 2, ... $e-1$ in gewisser Reihenfolge (mod. e) congruent, also stimmen die Perioden $\varepsilon_0, \varepsilon_1, \ldots \varepsilon_{e-1}$ mit den Perioden $\eta_0, \eta_1, \ldots \eta_{e-1}$, von der Ordnung abgesehen, überein, d. h., wenn man die primitive Wurzel g durch eine andere γ ersetzt, bleiben gleichwohl die Wurzeln, welche einer Periode angehörten, in einer der neuen Perioden beisammen.

Die e Perioden sind numerisch von einander verschieden. Wäre nämlich $\eta_h = \eta_k$, während h, k zwei verschiedene Zahlen aus der Reihe 0, 1, 2, ... $e-1$ bedeuten, so ergäbe sich die Gleichung:

$$r^{g^h} + r^{g^{h+e}} + \ldots + r^{g^{h+(f-1)e}} = r^{g^k} + r^{g^{k+e}} + \ldots + r^{g^{k+(f-1)e}},$$

welche nicht identisch ist, weil verschiedenen Perioden auch verschiedene Einheitswurzeln angehören. Indem man statt der Exponenten ihre kleinsten Reste (mod. p) substituirt und durch r dividirt, was möglich ist, da keine der Potenzen gleich Eins ist, erhält man eine nicht identische Gleichung von einem Grade, der höchstens $p-2$ beträgt, welche mit der irreductibeln Gleichung (1) vom Grade $p-1$ eine Wurzel r gemeinsam hat, was nicht sein kann.

5. Jede ganze Function von den Wurzeln der Gleichung (1), welche bei der Substitution von r^{g^e} an Stelle von r ungeändert bleibt, lässt sich als lineare Function der Perioden $\eta_0, \eta_1, \ldots \eta_{e-1}$ darstellen, in welcher die Coëfficienten ganze und ganzzahlige Func-

tionen von den gegebenen Coëfficienten sind, wenn diese entweder rationale Zahlen oder rationale Functionen von α sind.

Denken wir uns nämlich die gegebene Function in der Normalform (6):

$$f(r) = a_0 r + a_1 r^g + a_2 r^{g^2} + \ldots + a_{p-2} \cdot r^{g^{p-2}}.$$

Da nach der Voraussetzung $f(r) = f(r^{g^e})$, also auch

$$= f(r^{g^{2e}}) \ldots = f(r^{g^{(f-1)e}})$$

sein soll, so ist

$$f(r) = \frac{1}{f} [f(r) + f(r^{g^e}) + \ldots + f(r^{g^{(f-1)e}})].$$

Bildet man nun die Summe in der Klammer, so geht aus dem allgemeinen Gliede $a_h \cdot r^{g^h}$ der Function $f(r)$ der Ausdruck $\frac{a_h}{f} \cdot \eta_h$ hervor, also wird:

$$f(r) = \frac{1}{f} (a_0 \eta_0 + a_1 \eta_1 + \ldots + a_{p-2} \cdot \eta_{p-2})$$

oder, indem man die gleichen Perioden zusammenfasst,

$$f(r) = m_0 \eta_0 + m_1 \eta_1 + \ldots + m_{e-1} \cdot \eta_{e-1}.$$

Hierin sind $m_0, m_1, \ldots m_{e-1}$ ganze Functionen der gegebenen Coëfficienten, von denen nach der Herleitung klar ist, dass sie rationale Coëfficienten haben müssen. Diese müssen aber sogar ganzzahlig sein, denn die Coëfficienten in der Normalform, mit welcher nach Nr. 3 der vorige Ausdruck identisch sein muss, sind ebenfalls ganze Zahlen.

6. Aus diesem Satze ergeben sich unmittelbar einige wichtige Folgerungen.

1) Zunächst ist jedes Product aus zwei oder mehreren, gleichen oder verschiedenen der Perioden η_0, $\eta_1, \ldots \eta_{e-1}$, allgemeiner jede ganze Function der Perioden als eine lineare Function derselben darstellbar, mit Coëfficienten, welche ganze oder rationale Zahlen sind, entsprechend den Coëfficienten der ganzen Function. Denn alle diese Functionen fallen offenbar unter den vorigen Satz, da die Perioden selbst durch die Substitution von r^{g^e} für r unverändert bleiben.

Das Product aus zwei Perioden, $\eta_h \cdot \eta_k$, bringt man

leicht auf die angegebene Form, wenn man, wie folgt, verfährt: Da

$$\eta_h = r^{g^h} + r^{g^{h+e}} + \ldots + r^{g^{h+(f-1)e}}$$
$$\eta_k = r^{g^k} + r^{g^{k+e}} + \ldots + r^{g^{k+(f-1)e}}$$

ist, so kann man schreiben: $\eta_h \cdot \eta_k$

$$= r^{g^k}(r^{g^h} + r^{g^{h+e}} + \ldots + r^{g^{h+(f-1)e}})$$
$$+ r^{g^{k+e}}(r^{g^{h+e}} + r^{g^{h+2e}} + \ldots + r^{g^{h+e+(f-1)e}})$$
$$+ \ldots \ldots \ldots \ldots \ldots \ldots$$
$$+ r^{g^{k+(f-1)e}}(r^{g^{h+(f-1)e}} + r^{g^{h+fe}} + \ldots + r^{g^{h+2(f-1)e}}).$$

In dieser Summe geben die Glieder der ersten Verticalreihe:

$$r^{g^k+g^h} + r^{(g^k+g^h)g^e} + r^{(g^k+g^h)g^{2e}} + \ldots + r^{(g^k+g^h)g^{(f-1)e}};$$

ist also $g^k + g^h$ nicht durch p theilbar, so erhält man eine der f-gliedrigen Perioden, wenn dagegen $g^k + g^h$ durch p theilbar ist, wird der Werth dieser Verticalreihe gleich f, wofür man indessen auch $-f(\eta_0 + \eta_1 + \ldots + \eta_{e-1})$ substituiren kann, da die Summe $\eta_0 + \eta_1 + \ldots + \eta_{e-1}$ gleich der Summe aller Wurzeln der Gleichung (1) d. i. gleich -1 ist. Führt man diese Reduction an allen Verticalreihen aus, so erhält man den Ausdruck des Products $\eta_h \cdot \eta_k$ als lineare Function aller f-gliedrigen Perioden. (S. weiter unten Vorlesung 15, Nr. 1.)

2) **Jede ganze Function von den Wurzeln der Gleichung (1) mit ganzzahligen Coëfficienten, welche sich bei der Substitution von r^g an Stelle von r nicht ändert, hat einen ganzzahligen Werth.** In der That, setzt man im Satze der vorigen Nr. $e = 1$ also $f = p - 1$, so existirt nur die einzige Periode

$$\eta_0 = r + r^g + r^{g^2} + \ldots + r^{g^{p-2}},$$

deren Werth gleich -1 ist; durch diese kann aber jene Function linear ausgedrückt werden mit ganzzahligen Coëfficienten, wird also einer ganzen Zahl gleich.

3) **Jede ganze symmetrische Function der e f-gliedrigen Perioden $\eta_0, \eta_1, \ldots \eta_{e-1}$ ist einer ganzen Zahl gleich, wenn ihre Coëfficienten ganzzahlig sind.** Dies folgt aus der letzten Bemerkung; denn da bei der Substitution von r^g anstatt r die Perioden sich nur cyclisch unter einander

vertauschen, bleibt die symmetrische Function derselben dabei ungeändert.

7. **Mit Hilfe der vorigen Sätze können wir nun beweisen, dass die Perioden $\eta_0, \eta_1, \ldots \eta_{e-1}$ von f Gliedern die Wurzeln einer irreductibeln Gleichung vom Grade e sind, welche ganzzahlige Coëfficienten hat. Diese Gleichung hat mit der Kreistheilungsgleichung die Eigenschaft gemein, dass alle ihre Wurzeln aus einer beliebigen unter ihnen durch Wiederholung ein- und derselben rationalen Operation gebildet werden können.**

Die in Frage stehende Gleichung ist die folgende:

$$(7) \qquad F(x) = (x - \eta_0)(x - \eta_1) \ldots (x - \eta_{e-1}) = 0.$$

Ihre Coëfficienten sind ganze, ganzzahlige und symmetrische Functionen der e Perioden, also nach der letzten Bemerkung in voriger Nr. ganze Zahlen. Nehmen wir nun an, $F(x)$ sei reductibel und $F'(x)$ ein rationaler Factor von $F(x)$, so müsste wenigstens eine der Perioden, z. B. η_h diesem Factor als Wurzel zukommen, also $F'(\eta_h) = 0$ sein. Dies ist aber eine rationale Gleichung, welche mit der Gleichung (1) die Wurzel r gemein hat; nach der Irreductibilität der letztern kann man also r mit $r^g, r^{g^2}, \ldots r^{g^{e-1}}$ vertauschen und findet so:

$$F'(\eta_{h+1}) = 0, \ \ldots \ F'(\eta_{h-1}) = 0,$$

d. h. die Gleichung $F'(x) = 0$, deren Grad geringer als e sein muss, müsste die e verschiedenen Wurzeln $\eta_0, \eta_1, \ldots \eta_{e-1}$ haben, was nicht sein kann. Hiernach ist der erste Theil unsers Satzes bewiesen.

Um auch den andern Theil als richtig nachzuweisen, bemerken wir, dass nach Nr. 6, 1) jede Potenz einer beliebigen Periode η_h sich als lineare Function aller Perioden mit ganzzahligen Coëfficienten darstellen lässt. Es können also folgende Gleichungen aufgestellt werden:

$$\begin{aligned}
\eta_h &= \mu_0'\eta_0 + \mu_1'\eta_1 + \ldots + \mu'_{e-1} \cdot \eta_{e-1} \\
\eta_h^2 &= \mu_0''\eta_0 + \mu_1''\eta_1 + \ldots + \mu''_{e-1} \cdot \eta_{e-1} \\
& \ldots \ldots \ldots \ldots \ldots \ldots \\
\eta_h^{e-1} &= \mu_0^{(e-1)}\eta_0 + \mu_1^{(e-1)}\eta_1 + \ldots + \mu_{e-1}^{(e-1)} \cdot \eta_{e-1},
\end{aligned}$$

zu denen man noch die Gleichung

$$-1 = \eta_0 + \eta_1 + \ldots + \eta_{e-1}$$

hinzufügen mag, welche sich aus der Bemerkung ergiebt, dass die Summe aller Perioden gleich der Summe aller Wurzeln, diese letztere aber gleich — 1 ist. Nun kann man aus den e linearen Gleichungen eine beliebige Periode η_k bestimmen und findet nach dem gewöhnlichen Eliminationsverfahren eine Gleichung von der Form:

$$D \cdot \eta_k = A_0 + A_1 \eta_k + A_2 \eta_k^2 + \ldots + A_{e-1} \cdot \eta_k^{e-1},$$

in welcher die Coëfficienten ganze Zahlen sind, die nicht sämmtlich verschwinden, und woraus sich η_k durch Division mit D ergiebt. Denn D kann nicht Null sein, sonst bestünde die nicht identische Gleichung $(e-1)^{ten}$ Grades:

$$0 = A_0 + A_1 \eta_k + A_2 \eta_k^2 + \ldots + A_{e-1} \cdot \eta_k^{e-1},$$

während η_k eine Wurzel der irreductibeln Gleichung e^{ten} Grades $F(x) = 0$ ist.

Hiernach ist auch $\eta_1 = \vartheta(\eta_0)$, wo $\vartheta(\eta_0)$ eine gewisse ganze Function von η_0 bedeutet. Diese Gleichung kann aber als eine rationale Gleichung gedeutet werden, welcher die Wurzel r genügt, und muss bestehen bleiben, wenn man r durch $r^g, r^{g^2}, \ldots$ ersetzt; so findet man

$$\eta_2 = \vartheta(\eta_1), \; \eta_3 = \vartheta(\eta_2), \; \ldots \; \eta_{e-1} = \vartheta(\eta_{e-2}), \; \eta_0 = \vartheta(\eta_{e-1}),$$

womit Alles bewiesen ist, was unser Satz enthält.

Durch Auflösung der Gleichung (7) werden die e f-gliedrigen Perioden bekannt. Jedoch fragt es sich, wenn α eine bestimmte Wurzel der Gleichung (7) ist, welche der e Perioden sie ausdrücke. Nun ist aber r eine beliebige Wurzel der Kreistheilungsgleichung; wäre also bei einer bestimmten Wahl des r $\eta_k = \alpha$, so braucht man nur die Bedeutung von r zu verändern, nämlich eine beliebige derjenigen Wurzeln darunter zu verstehen, aus welchen η_k besteht, dann ändert sich auch die Bedeutung der Zeichen $\eta_0, \eta_1, \ldots \eta_{e-1}$, indem, was zuvor η_k war, nunmehr η_0 wird; man kann also bei passender Wahl von r immer setzen $\eta_0 = \alpha$, wobei die Wurzel r noch insoweit unbestimmt bleibt, als sie eine beliebige der Wurzeln sein kann, aus denen η_0 besteht, und welche nach Nr. 4 völlig bestimmt sind.

Hat man in dieser Weise die Periode η_0 bestimmt, so ergiebt sich der Werth der übrigen ohne weitere Auflösung anderer

als linearer Gleichungen, indem jede andere Periode nach den obigen Auseinandersetzungen rational durch η_0 ausgedrückt werden kann.

8. **Die f Wurzeln, aus denen eine Periode η_h besteht, leisten einer Gleichung f^{ten} Grades $\Phi_h(x) = 0$ Genüge, welche lineare und ganzzahlige Functionen der e Perioden $\eta_0, \eta_1, \ldots \eta_{e-1}$ zu Coëfficienten hat und in dem Sinne irreductibel ist, dass $\Phi_h(x)$ nicht in Factoren von gleicher Beschaffenheit zerlegt werden kann.**

Die Coëfficienten sind nämlich symmetrische Functionen der Wurzeln

(8) $$r^{g^h}, \; r^{g^{h+e}}, \; r^{g^{h+2e}}, \; \ldots \; r^{g^{h+(f-1)e}},$$

also unveränderlich, wenn diese in irgend einer Weise unter einander vertauscht werden. Nun ist aber die Substitution von r^{g^e} statt r einer cyclischen Vertauschung derselben äquivalent, also bleiben die Coëfficienten bei dieser Substitution unverändert und sind nach Nr. 5 lineare und ganzzahlige Functionen der f-gliedrigen Perioden. — Die gedachte Gleichung ist aber auch irreductibel. Wäre nämlich $f(x, \eta_0, \eta_1, \ldots \eta_{e-1})$ ein Factor von $\Phi_h(x)$ mit Coëfficienten, die ebenfalls lineare und ganzzahlige Functionen der Perioden $\eta_0, \eta_1, \ldots \eta_{e-1}$ sind, so müsste er wenigstens für eine der Wurzeln (8) verschwinden; man erhielte also, indem man den Perioden ihre Ausdrücke substituirt, eine Gleichung in r mit rationalen Coëfficienten, welche für sämmtliche Wurzeln der Kreistheilungsgleichung, z. B. für die übrigen in η_h enthaltenen bestehen bleiben müsste. Da die Perioden ungeändert bleiben, wenn man eine dieser Wurzeln für die andere setzt, so müssten der Gleichung

$$f(x, \eta_0, \eta_1, \ldots \eta_{e-1}) = 0$$

von geringerem Grade als f mindestens die f in η_h enthaltenen Wurzeln genügen, was nicht möglich ist.

Denken wir uns die e Gleichungen aufgestellt:

(9) $$\Phi_0(x) = 0, \; \Phi_1(x) = 0, \; \ldots \; \Phi_{e-1}(x) = 0,$$

so wird ihre Auflösung die vollständige Auflösung der Kreistheilungsgleichung ergeben. Es genügt sogar, eine einzige derselben aufzulösen, da man, wenn eine Wurzel der Kreistheilungsgleichung bekannt ist, durch ihre Potenzen alle übrigen findet. Um die

Gleichungen (9) aber bilden zu können, ist nothwendig und hinreichend, dass man zuvor die Gleichung (7) aufgelöst, nämlich die e f-gliedrigen Perioden bestimmt habe. Hiernach erhält man folgenden Satz:

Die Auflösung der Kreistheilungsgleichung vom Grade $p - 1 = e \,.\, f$ kommt darauf zurück, die Gleichung (7) vom Grade e und eine der Gleichungen (9) vom Grade f aufzulösen.

Dies lässt sich auch so aussprechen: Nach Auflösung der Gleichung (7) wird die Function X reductibel und zerfällt in e Factoren vom Grade f, welche bis auf Weiteres wieder irreductibel sind.

9. Man kann nun in ähnlicher Weise fortfahren. Zerlegt man f in die beiden Factoren e', f', so kann man ee' Perioden von f' Gliedern bilden:

$$\eta'_0 = r + r^{g^{ee'}} + r^{g^{2ee'}} + \ldots + r^{g^{(f'-1)ee'}}$$

$$\eta'_1 = r^g + r^{g^{ee'+1}} + r^{g^{2ee'+1}} + \ldots + r^{g^{(f'-1)ee'+1}}$$

$$\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot$$

$$\eta'_e = r^{g^e} + r^{g^{ee'+e}} + r^{g^{2ee'+e}} + \ldots + r^{g^{(f'-1)ee'+e}}$$

$$\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot$$

$$\eta'_{2e} = r^{g^{2e}} + r^{g^{ee'+2e}} + r^{g^{2ee'+2e}} + \ldots + r^{g^{(f'-1)ee'+2e}}$$

$$\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot$$

$$\eta'_{ee'-1} = r^{g^{ee'-1}} + r^{g^{2ee'-1}} + r^{g^{3ee'-1}} + \ldots + r^{g^{f'ee'-1}}.$$

Von diesen setzen je e' Perioden eine der f-gliedrigen zusammen, z. B. ist

$$\eta_0 = \eta'_0 + \eta'_e + \eta'_{2e} + \ldots + \eta'_{(e'-1)e},$$

und es gelten von ihnen dieselben Sätze, die wir von den f-gliedrigen Perioden bewiesen haben, mit den entsprechenden Modificationen. Besonders erwähnt sei nur der Satz, dass jede der f'-gliedrigen Perioden eine ganze rationale Function von irgend einer der übrigen ist.

Betrachten wir aber diejenigen e' Perioden, welche eine der f-gliedrigen zusammensetzen, z. B. die Perioden

$$(10) \qquad \eta'_0,\; \eta'_e,\; \eta'_{2e},\; \ldots\; \eta'_{(e'-1)e},$$

so genügen dieselben einer irreductibeln Gleichung

vom Grade e', deren Coëfficienten lineare Functionen der f-gliedrigen Perioden sind. Denn in der Gleichung

$$\Phi'_0(x) = (x - \eta'_0)(x - \eta'_e)(x - \eta'_{2e}) \ldots (x - \eta'_{(e'-1)e}) = 0$$

sind die Coëfficienten als symmetrische Functionen der Perioden (10) durch die Substitution von r^{g^e} statt r sicher unveränderlich, da durch dieselben die e' Perioden sich offenbar nur cyclisch vertauschen. Nach Nr. 5 folgt also, dass sie durch die f-gliedrigen Perioden ausdrückbar sind. Dass die Gleichung $\Phi'_0(x) = 0$ aber auch irreductibel ist, folgt aus der Irreductibilität der Gleichung $\Phi_0(x) = 0$. Wäre nämlich $\varphi(x, \eta_0, \eta_1, \ldots \eta_{e-1})$ ein Factor von $\Phi'_0(x)$ mit Coëfficienten, welche lineare Functionen der f-gliedrigen Perioden sind, so müsste er etwa für $x = \eta'_{he}$ verschwinden, also

$$\varphi(\eta'_{he}, \eta_0, \eta_1, \ldots \eta_{e-1}) = 0$$

sein. Diese Gleichung, aufgefasst als eine solche, welcher die eine Wurzel r der irreductibeln Gleichung $\Phi_0(x) = 0$ genügt, müsste befriedigt bleiben, wenn man r durch die Wurzeln r^{g^e}, $r^{g^{2e}}, \ldots r^{g^{(e'-1)e}}$ derselben ersetzt, wodurch zwar die Perioden $\eta_0, \eta_1, \ldots \eta_{e-1}$ unverändert bleiben, η'_{he} aber in $\eta'_{(h+1)e}, \ldots \eta'_{(h-1)e}$ successive übergeht. Die Gleichung hätte also mehr Wurzeln, als ihr Grad betragen kann.

Hiernach lassen sich, sobald durch Auflösung der Gleichung (7) die f-gliedrigen Perioden gefunden sind, e Gleichungen vom Grade e' aufstellen:

$$(11) \quad \Phi'_0(x) = 0,\ \Phi'_1(x) = 0,\ \Phi'_2(x) = 0, \ldots \Phi'_{e-1}(x) = 0,$$

deren jede je e' Perioden von f' Gliedern zu Wurzeln hat, und welche zur Bestimmung der f'-gliedrigen Perioden mittelst der f-gliedrigen dienen. Man hat nur nöthig, eine dieser Gleichungen aufzulösen, denn aus einer beliebigen der f'-gliedrigen Perioden ergeben sich die übrigen als rationale Functionen.

Wenn aber durch Auflösung einer der Gleichungen (11) vom Grade e' die f'-gliedrigen Perioden als bekannt anzusehen sind, so wird jeder der e Factoren f^{ten} Grades, in welche X bereits zerlegt war, von Neuem reductibel, und X zerfällt nach der vorigen Nr. in ee' Factoren vom Grade f', welche wieder zunächst irreductibel sind.

10. Durch Fortsetzung desselben Verfahrens muss man endlich dahin gelangen, dass X in Factoren ersten Grades zerfällt, und so die Wurzeln der Gleichung $X = 0$ unmittelbar bekannt werden. Hierin besteht die Gaussische Auflösungsmethode, welche in folgender Regel ihren Ausdruck findet: Man zerlege $p - 1$ in Factoren: $p - 1 = a \,.\, b \,.\, c \ldots d$, und vertheile alle Wurzeln der Gleichung $X = 0$ in a Perioden η von $\frac{p-1}{a}$ Gliedern. Diese leisten nach Nr. 7 einer Gleichung Genüge, welche ganzzahlige Coëfficienten hat. Durch Auflösung derselben werden die Perioden η bekannt, und zerfällt X in a Factoren vom Grade $\frac{p-1}{a}$, deren Coëfficienten durch die η ebenfalls bekannt sind. Nun vertheile man die Wurzeln jeder der Perioden η in b kleinere Perioden η' von $\frac{p-1}{ab}$ Gliedern. Diejenigen, welche eine der Perioden η zusammensetzen, genügen einer Gleichung vom Grade b, deren Coëfficienten linear durch die Perioden η ausdrückbar sind (nach Nr. 9). Nach Auflösung derselben werden alle ab Perioden η bekannt, und X zerfällt in ab Factoren vom Grade $\frac{p-1}{ab}$ mit bekannten Coëfficienten. Man vertheile nun wieder die Wurzeln jeder der Perioden η' in c kleinere Perioden η'' von $\frac{p-1}{abc}$ Gliedern; diejenigen, welche eine der Perioden η' zusammensetzen, sind (wieder nach Nr. 9) Wurzeln einer Gleichung vom Grade c, deren Coëfficienten linear durch die Perioden η' ausdrückbar sind. Nach deren Auflösung werden alle abc Perioden η'' bekannt, und X zerfällt in abc Factoren vom Grade $\frac{p-1}{abc}$ mit bekannten Coëfficienten u. s. w. Endlich kommt man auf Perioden von je einem Gliede d. h. auf einzelne Wurzeln der Gleichung $X = 0$, von welchen je d eine nächst vorhergehende Periode zusammensetzen und durch eine Gleichung vom Grade d bestimmt werden, deren Coëfficienten durch die nächst vorhergehenden Perioden ausdrückbar sind, und deren Auflösung die Wurzeln der Kreistheilungsgleichung selbst ergiebt.

Die Auflösung der Kreistheilungsgleichung kommt nach dieser Regel darauf zurück, je eine Gleichung vom Grade a, b, c, $\ldots$ d aufzulösen.

11. Wie man $p - 1$ in Factoren zerlege, ist zwar willkürlich; will man jedoch, dass die Hilfsgleichungen möglichst niedrigen Grad erhalten, so muss man $p - 1$ in seine einzelnen, gleichen oder ungleichen, Primfactoren zerlegen. Geschieht es dabei, dass alle Primfactoren gleich Zwei sind, d. h. ist p von der Form $2^k + 1$, so werden alle Hilfsgleichungen vom 2ten Grade und ihre Wurzeln durch Quadratwurzeln ausdrückbar. Da man nun jeden Ausdruck, welcher ausser Quadratwurzeln keine Irrationalitäten enthält, bekanntlich mit Hilfe von Cirkel und Lineal geometrisch construiren kann, so gilt dasselbe von den Wurzeln der Kreistheilungsgleichung und es ergiebt sich der Satz:

Ist p eine Primzahl von der Form $2^k + 1$, so kann der Kreis in p gleiche Theile getheilt oder ein regelmässiges Vieleck von p Seiten in den Kreis eingeschrieben werden allein mit Hilfe von Cirkel und Lineal.

Die in der ersten Vorlesung betrachteten Fälle des regelmässigen Dreiecks und Fünfecks gehören in die eben bezeichnete Kategorie.

Man wird gut thun, als letzten Factor der Zerlegung die Zwei zu nehmen, welche in der geraden Zahl $p - 1$ stets enthalten ist. Dann enthält nämlich jede der Perioden eine gerade Anzahl Glieder und besteht aus einer Summe der letzten zweigliedrigen Perioden:

$$r + r^{g^{\frac{p-1}{2}}},\; r^g + r^{g^{\frac{p-1}{2}+1}},\; r^{g^2} + r^{g^{\frac{p-1}{2}+2}},\; \ldots\; r^{g^{\frac{p-3}{2}}} + r^{g^{\frac{p-3}{2}+\frac{p-1}{2}}}$$

d. i. weil $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ gefunden wurde (Nr. 10 der 4. Vorlesung):

$$r + r^{-1},\; r^g + r^{-g},\; r^{g^2} + r^{-g^2},\; \ldots\; r^{g^{\frac{p-3}{2}}} + r^{-g^{\frac{p-3}{2}}}.$$

Diese sind sämmtlich reell; denn, ist $r = \cos \frac{2k\pi}{p} + i \sin \frac{2k\pi}{p}$, so ist

$$r^{g^h} = \cos \frac{2kg^h \cdot \pi}{p} + i \sin \frac{2kg^h \cdot \pi}{p}$$

$$r^{-g^h} = \cos \frac{2kg^h \cdot \pi}{p} - i \sin \frac{2kg^h \cdot \pi}{p}$$

also

$$r^{g^h} + r^{-g^h} = 2 \cdot \cos \frac{2 k g^h \cdot \pi}{p}.$$

Man gewinnt also den Vortheil, dass die Wurzeln aller Hilfsgleichungen reell sind, bis man durch Auflösung der letzten quadratischen Gleichung von den zweigliedrigen Perioden zu den imaginären Wurzeln der Kreistheilungsgleichung selber herabsteigt.

Erinnern wir uns hier, dass nach Nr. 7 und 9 die Hilfsgleichungen sämmtlich irreductibel sind und die Eigenschaft haben, dass jede ihrer Wurzeln eine rationale Function jeder der übrigen ist. Es liesse sich sogar zeigen, dass die Eigenschaft der Gleichung (7), nach welcher alle Wurzeln durch Wiederholung derselben rationalen Operation aus einer unter ihnen gebildet werden können, auch den übrigen Hilfsgleichungen zukommt. Diese Eigenschaft aber, verbunden mit der Irreductibilität, sichert, wie Abel in der bereits in der vorigen Vorlesung citirten Abhandlung gezeigt hat, indem er die Gaussischen Betrachtungen verallgemeinerte, den Gleichungen die algebraische Auflösbarkeit. Die Kreistheilungsgleichung $X = 0$ ist demnach auch algebraisch auflösbar, wie auch daraus hervorgeht, dass ihr nach Nr. 1 und nach der vorigen Vorlesung dieselben beiden characteristischen Eigenschaften zukommen. Um diesen Schluss zu ziehen, ist es indessen nicht nothwendig, die genannte Eigenschaft auch für die Hilfsgleichungen nachzuweisen. Nach derselben Abhandlung von Abel genügt es für ihre algebraische Auflösbarkeit, dass sie irreductibel und ihre Wurzeln rational durch eine unter ihnen ausdrückbar sind, vorausgesetzt, dass ihr Grad eine Primzahl ist, was man stets dadurch erreichen kann, dass man $p - 1$ in seine Primfactoren zerlegt denkt.

Wir werden bald die algebraische Auflösbarkeit all' der eben genannten Gleichungen durch eine directe Methode nachweisen. In der nächsten Vorlesung sollen jedoch zuvor einige Beispiele für die eben dargestellte Auflösungsmethode wirklich berechnet werden.

Siebente Vorlesung.

Beispiele.

1. Um die allgemeine Gaussische Methode zur Auflösung der Kreistheilungsgleichung an einigen Beispielen zu erläutern, wählen wir zunächst für p die Primzahl 5.

In diesem Falle ist $p - 1 = 2 . 2$, man wird also nur successive zwei quadratische Gleichungen aufzulösen haben. Vor Allem kommt es darauf an, eine primitive Wurzel g (mod. 5) zu finden; man überzeugt sich aber sofort, dass $g = 2$ eine solche ist. Da dann den Potenzen

$$1, \quad g, \quad g^2, \quad g^3$$

oder den Indices

$$0, \quad 1, \quad 2, \quad 3$$

die Zahlen

$$1, \quad 2, \quad 4, \quad 3$$

entsprechen, so vertheilen sich die vier Wurzeln r, r^2, r^3, r^4 der Gleichung

$$(1) \qquad \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1 = 0$$

in die beiden Perioden

$$\eta_0 = r + r^4, \quad \eta_1 = r^2 + r^3,$$

welche Wurzeln der quadratischen Gleichung

$$x^2 - (\eta_0 + \eta_1)x + \eta_0\eta_1 = 0$$

sind. Nun findet man aber

$$\eta_0 + \eta_1 = r + r^2 + r^3 + r^4$$

d. i. gleich der Summe aller Wurzeln der Gleichung (1), also gleich -1,

$$\eta_0\eta_1 = (r + r^4)(r^2 + r^3) = r^3 + r^2 + r + r^4 = -1,$$

die quadratische Gleichung nimmt daher die Form an:

$$x^2 + x - 1 = 0$$

und hat die Wurzeln

$$\frac{-1 + \sqrt{5}}{2}, \quad \frac{-1 - \sqrt{5}}{2},$$

von denen man nach Belieben die eine gleich η_0, die andere gleich η_1, z. B.

$$\eta_0 = \frac{-1+\sqrt{5}}{2}, \quad \eta_1 = \frac{-1-\sqrt{5}}{2}$$

setzen kann (s. die Bemerkung in Nr. 7 der vorigen Vorlesung), indem man die beliebige Wurzel r passend gewählt denkt, nämlich als eine der Wurzeln derjenigen Periode, welche eben den Werth $\frac{-1+\sqrt{5}}{2}$ hat.

Bestimmen wir nun die Gleichung, welcher die beiden in η_0 enthaltenen Wurzeln r und r^1 Genüge leisten. Diese ist

$$x^2 - (r + r^4)x + r \cdot r^4 = 0$$

oder

$$x^2 - \eta_0 x + 1 = 0,$$

und ihre Auflösung giebt die Wurzeln r und r^4. Man darf setzen

$$r = \frac{\eta_0}{2} + \sqrt{\frac{\eta_0^2}{4} - 1},$$

ein Ausdruck, der durch Substitution des Werthes von η_0 die Gestalt annimmt:

$$r = \frac{-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}}{4}.$$

Von den beiden Werthen η_0, η_1 ist offenbar der erstere positiv, der zweite negativ. Da nun, wenn $r = \cos\frac{2k\pi}{5} + i\sin\frac{2k\pi}{5}$ gesetzt wird, η_0 und η_1 in $2\cos\frac{2k\pi}{5}$ und $2\cos\frac{4k\pi}{5}$ resp. übergehen, wird man $k = 1$ oder $k = 4$ wählen müssen, um der getroffenen Wahl von η_0 zu genügen. Man darf also

$$r = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5} \quad \text{und} \quad \eta_0 = 2\cos\frac{2\pi}{5}$$

setzen.

Die Aufgabe, den Kreis in fünf gleiche Theile zu theilen, gestattet nach Nr. 11 der vorigen Vorlesung eine Lösung mittels Cirkel und Lineal. Man kann z. B. folgendermassen verfahren. In dem zu theilenden Kreise (Fig. 1) werde der Radius als Einheit genommen, zwei auf einander senkrechte Durchmesser AB, CD und in A, D die Tangenten gezogen, welche sich in S schnei-

den; man halbire AS in E und verbinde E mit dem Mittelpunkte O des Kreises, so ist

$$OE = \sqrt{OA^2 + AE^2} = \tfrac{1}{2}\sqrt{5}.$$

Schlägt man nun mit OE um E einen Kreis, der AS in F trifft, so ist

$$AF = \tfrac{1}{2}\sqrt{5} - \tfrac{1}{2} = \eta_0 = 2\cos\frac{2\pi}{5}$$

folglich

$$AG = \cos\frac{2\pi}{5},$$

wenn man durch die Parallele OG zu BF die Strecke AF in G halbirt. Die Parallele GHJ zu AB schneidet demnach den Kreis in zwei Punkten H, J, von denen jeder ein Eckpunkt des Fünfecks ist, welches man erhält, indem man CH oder CJ zu wiederholten Malen in die Kreisperipherie einträgt.

Fig. 1.

F G A E S H C J B O D

2. Als zweites Beispiel wählen wir den Fall $p = 13$. In diesem ist $p - 1 = 3.2.2$, die Auflösung der Gleichung

$$\frac{x^{13} - 1}{x - 1} = 0$$

kommt also nach Gauss' allgemeiner Methode darauf zurück, successive eine cubische und zwei quadratische Gleichungen aufzulösen. Bei der Wahl der Zahl 6 als primitive Wurzel (mod. 13) findet man die Indices

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11,

und die Zahlen

1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11

einander entsprechend. Sind nun zunächst η_0, η_1, η_2 die drei Perioden von $\frac{p-1}{3} = 4$ Gliedern, so erhält man

$$\eta_0 = r + r^8 + r^{12} + r^5, \quad \eta_1 = r^6 + r^9 + r^7 + r^4,$$
$$\eta_2 = r^{10} + r^2 + r^3 + r^{11}$$

als Wurzeln der cubischen Gleichung:

$$x^3 - (\eta_0 + \eta_1 + \eta_2)\, x^2 + (\eta_0\eta_1 + \eta_1\eta_2 + \eta_2\eta_0)\, x - \eta_0\eta_1\eta_2 = 0.$$

Zunächst ist nun wieder der erste Coëfficient

$$\eta_0 + \eta_1 + \eta_2 = -1.$$

Die beiden andern Coëfficienten der Gleichung aber ergeben sich leicht, wenn man die in Nr. 6, 1 der vorigen Vorlesung angegebene Methode zur Multiplication zweier Perioden benutzt. Hiernach findet man nämlich die Gleichungen:

$$\eta_0\eta_1 = 2\eta_0 + \eta_1 + \eta_2$$
$$\eta_1\eta_2 = \eta_0 + 2\eta_1 + \eta_2$$
$$\eta_2\eta_0 = \eta_0 + \eta_1 + 2\eta_2$$
$$\eta_0\eta_0 = 4 + 2\eta_1 + \eta_2$$

und daraus

$$\eta_0\eta_1 + \eta_1\eta_2 + \eta_2\eta_0 = 4\,(\eta_0 + \eta_1 + \eta_2) = -4,$$
$$\eta_0\eta_1\eta_2 = \eta_0\eta_0 + 2\eta_0\eta_1 + \eta_0\eta_2 = -1.$$

Die cubische Gleichung erhält daher die Gestalt:

$$x^3 + x^2 - 4x + 1 = 0.$$

Nachdem man dieselbe aufgelöst hat, was bekanntlich stets möglich ist, sind η_0, η_1, η_2 als bekannt anzusehen und nunmehr in die sechs kleineren Perioden η' von nur zwei Gliedern zu zerlegen. So zerfällt η_0 in die beiden Perioden

$$\eta'_0 = r + r^{12}, \quad \eta'_3 = r^8 + r^5,$$

welche die Gleichung

$$x^2 - (\eta'_0 + \eta'_3)\, x + \eta'_0\eta'_3 = 0$$

befriedigen. Da in dieser

$$\eta'_0 + \eta'_3 = \eta_0 \text{ und } \eta'_0\eta'_3 = \eta_1$$

gefunden wird, nimmt sie die Form an:

$$x^2 - \eta_0 x + \eta_1 = 0$$

und lässt nun durch Auflösung die Perioden η'_0, η'_3 finden. Nachdem dies geschehen, bilde man endlich die quadratische Gleichung

$$x^2 - (r + r^{12})\, x + r \,.\, r^{12} = 0$$

mit den Wurzeln r, r^{12}, aus denen die Periode η'_0 besteht, und welche so geschrieben werden kann:

$$x^2 - \eta'_0 x + 1 = 0,$$

und durch die bekannte Auflösungsregel der quadratischen Gleichungen zur Kenntniss der gesuchten Grösse r führt.

3. Wir wollen endlich $p = 17$ annehmen, also die Aufgabe stellen, in den Kreis ein regelmässiges Siebenzehneck einzutragen.

Die Aufgabe kommt darauf zurück, die Gleichung

$$\frac{x^{17} - 1}{x - 1} = 0$$

aufzulösen. Nach der Gaussischen Methode müssen vor Allem die Perioden gebildet werden, und dazu ist die Wahl einer primitiven Wurzel g für den Modulus 17 nothwendig. Eine solche ist aber $g = 3$ und zwar entsprechen den Potenzen

$$1,\, g,\, g^2,\, g^3,\, g^4,\, g^5,\, g^6,\, g^7,\, g^8,\, g^9,\, g^{10},\, g^{11},\, g^{12},\, g^{13},\, g^{14},\, g^{15}$$

oder den Indices

$$0,\, 1,\, 2,\, 3,\, 4,\, 5,\, 6,\, 7,\, 8,\, 9,\, 10,\, 11,\, 12,\, 13,\, 14,\, 15,$$

hier die Zahlen

$$1,\, 3,\, 9,\, 10,\, 13,\, 5,\, 15,\, 11,\, 16,\, 14,\, 8,\, 7,\, 4,\, 12,\, 2,\, 6$$

als kleinste positive Reste jener Potenzen von $g = 3$ (mod. 17).

Man zerlege nun $p - 1 = 16$ in die vier Factoren $2.2.2.2$. Bildet man dann zuerst zwei Perioden η_0, η_1 von acht Gliedern, so findet man

$$\eta_0 = r + r^9 + r^{13} + r^{15} + r^{16} + r^8 + r^4 + r^2,$$
$$\eta_1 = r^3 + r^{10} + r^5 + r^{11} + r^{14} + r^7 + r^{12} + r^6.$$

Diese sind die Wurzeln der quadratischen Gleichung

$$x^2 - (\eta_0 + \eta_1)\, x + \eta_0\eta_1 = 0.$$

Es ergiebt sich sofort $\eta_0 + \eta_1$ als Summe aller Wurzeln der Gleichung

$$x^{16} + x^{15} + x^{14} + \ldots + x^2 + x + 1 = 0$$

gleich -1. Für das Product der beiden Perioden aber findet man nach der in Nr. 6, 1) der vorigen Vorlesung angegebenen Multiplicationsmethode leicht den Werth

$$\eta_0\eta_1 = 4\,(\eta_0 + \eta_1) = -4.$$

Die Perioden η_0, η_1 sind also die Wurzeln der Gleichung

$$x^4 + x - 4 = 0,$$

d. i. gleich

$$\frac{-1+\sqrt{17}}{2} \quad \text{und} \quad \frac{-1-\sqrt{17}}{2}.$$

Man darf einen beliebigen dieser Werthe mit η_0, den andern mit η_1 bezeichnen, also z. B.

$$(2) \qquad \eta_0 = \frac{-1+\sqrt{17}}{2}, \quad \eta_1 = \frac{-1-\sqrt{17}}{2}$$

setzen, indem man die Wurzel r passend gewählt denkt.

Nun zerlege man jede der achtgliedrigen Perioden in zwei kleinere von vier Gliedern:

$$\eta'_0 = r + r^{13} + r^{16} + r^4, \quad \eta'_1 = r^3 + r^5 + r^{14} + r^{12},$$
$$\eta'_2 = r^9 + r^{15} + r^8 + r^2, \quad \eta'_3 = r^{10} + r^{11} + r^7 + r^6.$$

Die Perioden η'_0, η'_2, welche die Periode η_0 zusammensetzen, ebenso die Perioden η'_1, η'_3, aus denen η_1 besteht, leisten je einer Gleichung zweiten Grades Genüge, deren Coëfficienten zwar nicht mehr rationale Zahlen, aber doch rational durch die Perioden η_0, η_1 ausdrückbar sind, nämlich den beiden Gleichungen

$$x^2 - (\eta'_0 + \eta'_2)\,x + \eta'_0\eta'_2 = 0, \quad x^2 - (\eta'_1 + \eta'_3)\,x + \eta'_1\eta'_3 = 0,$$

denen man leicht folgende Gestalt giebt:

$$x^2 - \eta_0 x - 1 = 0, \quad x^2 - \eta_1 x - 1 = 0.$$

Die Wurzeln der erstern sind:

$$x = \frac{\eta_0}{2} \pm \sqrt{\frac{\eta_0^2}{4} + 1},$$

die der zweiten:

$$x = \frac{\eta_1}{2} \pm \sqrt{\frac{\eta_1^2}{4} + 1},$$

und man darf setzen

$$(3) \qquad \eta'_0 = \frac{\eta_0}{2} + \sqrt{\frac{\eta_0^2}{4} + 1}, \quad \eta'_2 = \frac{\eta_0}{2} - \sqrt{\frac{\eta_0^2}{4} + 1}.$$

Um jedoch zu entscheiden, wie die Perioden η'_1, η'_3 den Wurzeln der zweiten Gleichung zugeordnet werden müssen, bedienen wir uns eines von Gauss angegebenen Hilfsmittels. Bildet man nämlich nach der bereits mehrfach erwähnten Methode das Product $(\eta'_0 - \eta'_2)\,(\eta'_1 - \eta'_3)$, so findet man die Gleichung

$$(\eta'_0 - \eta'_2)\,(\eta'_1 - \eta'_3) = 2\,(\eta_0 - \eta_1)$$

der:

$$+\sqrt{\frac{\eta_0^2}{4}+1}\,.\,(\eta'_1-\eta'_3)=+\sqrt{17};$$

da hiernach $\eta'_1 - \eta'_3$ positiv sein muss, so ist zu setzen:

$$(4)\qquad \eta'_1=\frac{\eta_1}{2}+\sqrt{\frac{\eta_1^2}{4}+1},\quad \eta'_3=\frac{\eta_1}{2}-\sqrt{\frac{\eta_1^2}{4}+1}.$$

Nun müssen die viergliedrigen Perioden weiter in die zweigliedrigen zerlegt werden, deren Ausdrücke sind:

$$\eta''_0=r+r^{16},\quad \eta''_1=r^3+r^{14},\quad \eta''_2=r^9+r^8,\quad \eta''_3=r^{10}+r^7,$$
$$\eta''_4=r^{13}+r^4,\quad \eta''_5=r^5+r^{12},\quad \eta''_6=r^{15}+r^2,\quad \eta''_7=r^{11}+r^6.$$

Diejenigen je zwei Perioden η'', welche eine Periode η' zusammensetzen, sind immer Wurzeln einer quadratischen Gleichung, deren Coëfficienten rational durch die Perioden η' ausgedrückt werden können. Alle diese Gleichungen lassen sich leicht bilden, und mit Hilfe des erwähnten Gaussischen Princips können auch ihre Wurzeln ohne jede Zweideutigkeit angegeben werden. Es genügt jedoch zu unserm Zwecke, eine einzige dieser Gleichungen zu betrachten, z. B. diejenige, deren Wurzeln η''_0, η''_4 sind, und für welche man findet

$$x^2-(\eta''_0+\eta''_4)\,x+\eta''_0\,.\,\eta''_4=0$$

oder

$$(5)\qquad x^2-\eta'_0x+\eta'_1=0.$$

Hieraus kann η''_0 bestimmt und gesetzt werden:

$$(6)\qquad \eta''_0=\frac{\eta'_0}{2}+\sqrt{\frac{\eta'^2_0}{4}-\eta'_1}.$$

Endlich gelangt man zur Kenntniss der Wurzel r selbst, indem man eine quadratische Gleichung auflöst, welche die, die Periode η''_0 bildenden Grössen r, r^{16} zu Wurzeln hat, nämlich die Gleichung

$$x^2-(r+r^{16})\,x+r\,.\,r^{16}=0$$

oder

$$x^2-\eta''_0\,x+1=0,$$

aus welcher

$$r=\frac{\eta''_0}{2}+\sqrt{\frac{\eta''^2_0}{4}-1}$$

sich ergiebt. —

4. Die Primzahl $p=17$ gehört wieder zu denjenigen, für welche die Theilung des Kreises allein durch Cirkel und Lineal ausführbar ist. Da die entwickelten Ausdrücke für die Wurzeln der Gleichung

$$\frac{x^{17}-1}{x-1}=0$$

ziemlich complicirt ausfallen, darf man freilich nicht erwarten, dass ihre Construction eine sehr einfache sei. Von den bekannten Constructionen des Siebenzehnecks soll hier mit leichten Modificationen diejenige reproducirt werden, welche sich in Serret's Handbuch der Algebra, deutsch von Werthheim, 2. Bd., pag. 442, findet, da sie den Gang der soeben ausgeführten Rechnungen am Deutlichsten hervortreten lässt. Auf eine andere von Staudt herrührende Construction im 24. Bd. des Crelle'schen J., pag. 251, wo auch eine solche für das Fünfeck angegeben wird, werden wir nachher zurückkommen.

Im Voraus mag bemerkt werden, dass nach den Formeln (2) die Periode η_0 positiv, η_1 aber negativ ist. Die Perioden η'_0, η'_1, η''_0 dagegen, von welchen die letzte gleich $2 \,.\, \cos\frac{2k\pi}{17}$ ist, wenn $r=\cos\frac{2k\pi}{17}+i\sin\frac{2k\pi}{17}$ gesetzt wird, erhalten positive Werthe.

Man ziehe nun (Fig. 2) in dem zu theilenden Kreise mit dem Radius 1 zwei auf einander senkrechte Durchmesser AB, CD und in A, D die Tangenten, die sich in S schneiden, und mache $AE=\frac{1}{4}AS$. Dann ist aus dem rechtwinkligen Dreiecke EAO:

$$OE=\sqrt{AO^2+AE^2}=\tfrac{1}{4}\sqrt{17}.$$

Beschreibt man sodann mit OE um E als Mittelpunkt einen Kreis, welcher AS in F und F' schneidet, so ist

$$AF=EF-EA=\frac{\sqrt{17}-1}{4}=\frac{\eta_0}{2},$$

$$AF'=EF'+EA=\frac{\sqrt{17}+1}{4}=-\frac{\eta_1}{2},$$

ferner aus den rechtwinkligen Dreiecken FAO und $F'AO$:

$$OF=\sqrt{AO^2+AF^2}=\sqrt{\frac{\eta_0^2}{4}+1},$$

$$OF'=\sqrt{AO^2+AF'^2}=\sqrt{\frac{\eta_1^2}{4}+1}.$$

Indem man daher um F als Mittelpunkt mit FO, und um F' als Mittelpunkt mit $F'O$ zwei Kreise schlägt, welche AS in H und H' treffen und die Strecke AH durch die zu BH gezogene Parallele OJ in J halbirt, findet man

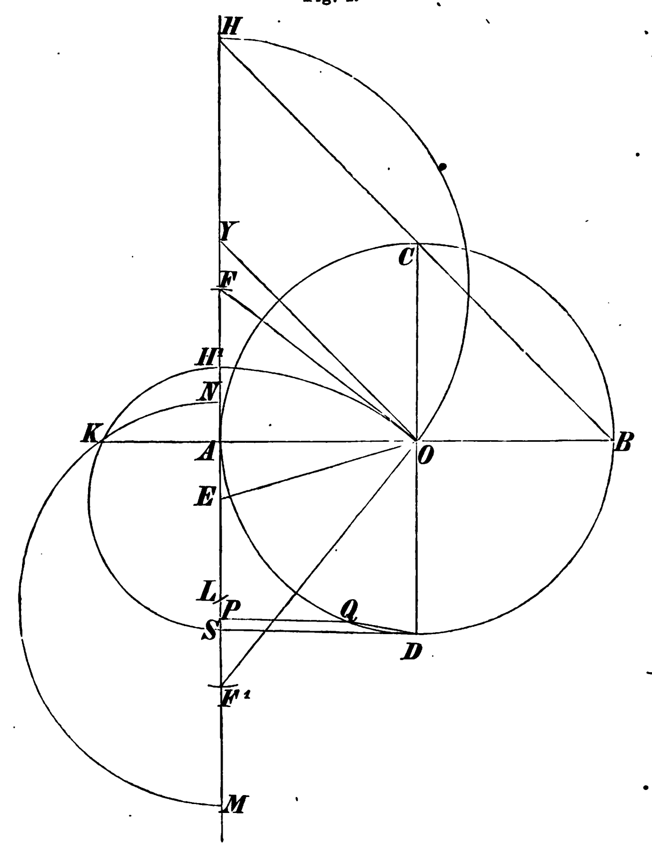
$$AH = FH + FA = FO + FA = \frac{\eta_0}{2} + \sqrt{\frac{\eta_0^2}{4} + 1} = \eta'_0,$$

$$AH' = F'H' - F'A = F'O - F'A = \frac{\eta_1}{2} + \sqrt{\frac{\eta_1^2}{4} + 1} = \eta'_1,$$

$$AJ = \frac{\eta'_0}{2}.$$

Nunmehr schlage man über $H'S$ einen Halbkreis und ver-

Fig. 2.



längere AB über A hinaus bis zum Durchschnitte K mit demselben; dann ist

$$AK^2 = AH' \cdot AS = \eta'_1.$$

Wenn man aber um K als Mittelpunkt mit dem Radius AJ einen Kreis schlägt, und von dem Schnittpunkte L desselben mit

der Geraden AS mit demselben Radius den Kreis MKN zieht, so ist auch

$$AK^2 = AM \,.\, AN,$$

also

$$AM \,.\, AN = \eta'_1,$$

während

$$AM + AN = 2 \,.\, AJ = \eta'_0$$

ist. Hiernach sind AM und AN die Wurzeln der quadratischen Gleichung (5) und AM als die grössere derselben nach Formel (6) gleich η''_0. Wenn also endlich P die Strecke AM halbirt, so ist $AP = \cos\frac{2k\pi}{17}$, und man braucht nur PQ mit AB parallel zu ziehen bis zum Durchschnitte mit dem gegebenen Kreise, um einen Eckpunkt Q des Siebzehnecks zu finden, welches man selber erhält, indem man DQ 17 Mal in die Kreisperipherie einträgt.

Den nächsten Fall, in welchem die Theilung des Kreises mittels Cirkel und Lineal möglich ist, würde die Primzahl $p = 257$ darbieten. Ueber die Auflösung der entsprechenden Gleichung $x^{257} = 1$ müssen wir hier auf Richelot's umfangreiche Arbeit in Crelle's J., Bd. 9, verweisen. Wenn übrigens die Gauss'sche Methode die nothwendige Form der Primzahlen liefert, für welche die Kreistheilung durch Cirkel und Lineal ausführbar ist, indem sie lehrt, dass $p = 2^m + 1$ sein müsse, so wird doch keineswegs jede Zahl dieser Form einen solchen Fall darbieten, da $2^m + 1$ nicht für jeden Werth von m eine Primzahl ist. Zunächst ist dazu erforderlich, dass m eine Potenz von 2 ist, denn, wäre es durch eine ungerade Zahl theilbar, etwa $m = m'(2n+1)$, so würde nach der Formel

$$x^{2n+1} + 1 = (x+1)\,(x^{2n} - x^{2n-1} + x^{2n-2} - \ldots + x^2 - x + 1)$$

$2^{m'(2n+1)} + 1$ durch $2^{m'} + 1$ theilbar, also eine zusammengesetzte Zahl sein. Aber dass auch nicht alle Zahlen von der Form $2^{2^n} + 1$ Primzahlen sind, lehrt die Annahme $n = 5$, denn die derselben entsprechende Zahl

$$2^{2^5} + 1 = 4294967297$$

enthält den Factor 641. Nach dieser Bemerkung bleibt es auch zweifelhaft, ob es unendlich viel Primzahlen giebt, für welche Cirkel und Lineal ausreichen, um die Theilung des Kreises zu bewerkstelligen. —

Anhang.

Als Anhang zu dieser Vorlesung will ich noch folgende, die v. Staudt'sche Construction des regulären Siebenzehnecks betreffende Mittheilung des Herrn Professor Schröter, welche er mir freundlichst zur Benutzung überlassen hat, hier beifügen, indem ich bis auf einige redactionelle Aenderungen ganz seiner Darstellung mich anschliesse.

1. Nach Nr. 3 der 7. Vorlesung kommt es allein darauf an, zuerst die Wurzeln der quadratischen Gleichung

$$x^2 + x - 4 = 0, \tag{1}$$

nämlich die beiden Perioden

$$\eta_0 = \frac{-1+\sqrt{17}}{2}, \quad \eta_1 = \frac{-1-\sqrt{17}}{2}, \tag{2}$$

sodann die Wurzeln jeder der beiden quadratischen Gleichungen

$$x^2 - \eta_0 x - 1 = 0, \quad x^2 - \eta_1 x - 1 = 0, \tag{3}$$

d. h. die Perioden

$$\eta'_0 = \frac{\eta_0}{2} + \sqrt{\frac{\eta_0^2}{4} + 1}, \quad \eta'_2 = \frac{\eta_0}{2} - \sqrt{\frac{\eta_0^2}{4} + 1} \tag{4}$$

einerseits, und die Perioden

$$\eta'_1 = \frac{\eta_1}{2} + \sqrt{\frac{\eta_1^2}{4} + 1}, \quad \eta'_3 = \frac{\eta_1}{2} - \sqrt{\frac{\eta_1^2}{4} + 1} \tag{5}$$

andererseits, endlich die Periode

$$\eta''_0 = \frac{\eta'_0}{2} + \sqrt{\frac{\eta'^2_0}{4} - \eta'_1}, \tag{6}$$

welche gleich $2\cos\frac{2k\pi}{17}$ ist und die quadratische Gleichung

$$x^2 - \eta'_0 x + \eta'_1 = 0 \tag{7}$$

befriedigt, zu construiren. Es handelt sich also um die geometrische Construction der Wurzeln quadratischer Gleichungen, und diese kann stets vermittelst der Durchschnittspunkte einer geraden Linie mit einem Kreise in folgender Weise ausgeführt werden:

Nehmen wir zwei parallele Tangenten eines Kreises mit dem Radius 1 (s. d. Tafel Fig. 1), welche in den Endpunkten eines Durchmessers CD berühren, und möge eine beliebige Transversale den Kreis in den Punkten E, E_1, die beiden parallelen Tangenten in

den Punkten c und d treffen; ziehen wir die Linien CE, CE_1, welche Dd in e und e_1 treffen, ebenso DE, DE_1, welche Cc in ε und ε_1 begegnen, so bestehen zwischen den auf den beiden parallelen Tangenten abgeschnittenen Stücken einfache Beziehungen, welche wir ermitteln wollen.

Da die Polare von c durch C und den vierten harmonischen Punkt zu c, E, E_1 gehen muss, so wird sie die Tangente Dd in einem solchen Punkte m treffen, welcher zu e, e_1 und dem unendlich entfernten Punkte harmonisch liegt, d. h. m wird die Mitte von ee_1 sein, und wir haben also

$$\tfrac{1}{2}(De + De_1) = Dm.$$

Weil aber die Polare von c senkrecht steht auf cM, so sind die Dreiecke cCM und CDm ähnlich, also

$$Cc : CM = DC : Dm, \text{ d. h. } Dm = \frac{2}{Cc},$$

also

$$De + De_1 = \frac{4}{Cc}. \tag{8}$$

In gleicher Weise erhalten wir andererseits

$$C\varepsilon + C\varepsilon_1 = \frac{4}{Dd}.$$

Es sind aber die Dreiecke εCD und CDe ähnlich, da Ce auf DE oder $D\varepsilon$ senkrecht steht, also ist

$$C\varepsilon : CD = DC : De, \text{ d. h. } C\varepsilon = \frac{4}{De},$$

und ebenso

$$C\varepsilon_1 = \frac{4}{De_1},$$

also folgt

$$\frac{1}{De} + \frac{1}{De_1} = \frac{1}{Dd}$$

und hieraus, nach der Beziehung (8):

$$De \,.\, De_1 = \frac{4\,Dd}{Cc}. \tag{9}$$

Fassen wir nun De und De_1 als Wurzeln der quadratischen Gleichung

$$x^2 - px + q = 0, \tag{10}$$

so werden deren Coëfficienten p, q als Summe und Product der Wurzeln durch die Gleichungen (8) und (9) bekannt, nämlich

$$(11) \qquad p = \frac{4}{Cc}, \quad q = \frac{4\,Dd}{Cc}$$

sein.

Umgekehrt, wenn die Gleichung (10) gegeben ist, so construirt man ihre Wurzeln, indem man aus den Gleichungen (11) auf den parallelen Tangenten in C und D zwei Punkte c und d bestimmt, deren Verbindungslinie den Kreis in solchen zwei Punkten E, E_1 trifft, welche, mit C verbunden, auf der Tangente in D die gesuchten Wurzeln als die Abschnitte De und De_1 liefern.

Was die Realität der Wurzeln anbetrifft, so ist die Bedingung dafür auch geometrisch leicht zu fixiren. Offenbar werden die beiden Schnittpunkte E, E_1 reell sein, wenn das abgeschnittene Stück Dd kleiner ist als dasjenige Stück $D\delta$, welches die zweite, aus c an den Kreis gelegte Tangente auf Dd abschneidet; und da $D\delta = \frac{1}{Cc}$ ist, so folgt als Bedingung für reelle Schnittpunkte:

$$Cc \,.\, Dd < 1.$$

Liegen also c und d nach entgegengesetzten Richtungen hin auf den beiden parallelen Tangenten, so werden die Wurzeln immer reell sein, weil das Product $Cc \,.\, Dd$ negativ wird; liegen sie nach gleichen Richtungen hin, so werden die Wurzeln nur dann reell sein, wenn das Rechteck aus den beiden Abschnitten Cc, Dd kleiner als das Quadrat des Kreisradius ist. —

2. Auf Grund dieser allgemeinen Betrachtungen lassen sich nun die Wurzeln der quadratischen Gleichungen (1), (3) und (7) successive construiren (s. Fig. 2).

Für die erste dieser Gleichungen hat man

$$\eta_0 + \eta_1 = -1, \quad \eta_0\eta_1 = -4;$$

vergleichen wir diese Relationen mit den Gleichungen (8) und (9), so haben wir $Cc = -4$, $Dd = +4$ zu setzen. Wir tragen also auf die Tangente in C nach einer Seite hin das Stück Cc gleich dem doppelten Durchmesser des Kreises, auf der Tangente in D nach der entgegengesetzten Seite hin das gleiche Stück Dd ab, ziehen cd, welche Linie den Kreis in E und E_1 treffe, und ziehen CE, CE_1, welche Dd in e und e_1 treffen; dann sind De und De_1 die Wurzeln unserer ersten quadratischen Gleichung,

und zwar wird, wenn wir Cc als die negative, Dd als die positive Richtung auffassen, De die positive, De_1 die negative Wurzel, also

$$De = \eta_0, \quad De_1 = \eta_1$$

sein.

Die zweite aufzulösende quadratische Gleichung ist in den Formeln enthalten:

$$\eta'_0 + \eta'_2 = \eta_0, \quad \eta'_0 \cdot \eta'_2 = -1,$$

und dies zu vergleichen mit den Relationen (8) und (9) oder, indem wir, um Verwechselung zu vermeiden, c' und d' an Stelle von c und d setzen und zugleich f und f_2 anstatt der früheren Buchstaben e und e_1, mit den folgenden Gleichungen:

$$Df + Df_2 = \frac{4}{Cc'} = De, \quad Df \cdot Df_2 = \frac{4\,Dd'}{Cc'} = -1.$$

Hieraus ist zunächst c' leicht zu finden, da $\frac{4}{Cc'} = De$, also $Cc' = \frac{4}{De}$ ist. Wir haben nur nöthig, DE zu ziehen, welches die Tangente in C in dem gesuchten Punkte c' treffen muss.

Um den zweiten Punkt d' zu finden, bemerken wir, dass, wenn $c'd'$ den Durchmesser CD in p trifft,

$$Cc' : Dd' = Cp : Dp$$

sein muss, also

$$\frac{Cp}{Dp} = \frac{-4}{1} = \frac{Cc}{1},$$

wodurch der Punkt p bestimmt wird; wir tragen auf die Tangente in D nach der positiven Seite den Radius des Kreises gleich DJ auf, ziehen Jc, welches in p den Durchmesser CD trifft, dann wird $c'p$ den Kreis in zwei Punkten F und F_2 treffen, CF und CF_2 aber die Tangente in D in den Punkten f und f_2, sodass Df und Df_2 die gesuchten Wurzeln sind; und da Df positiv, Df_2 negativ zu schätzen ist, findet sich

$$Df = \eta'_0, \quad Df_2 = \eta'_2.$$

In ganz gleicher Weise ermitteln wir die Wurzeln der zweiten Gleichung (3) aus den Relationen

$$\eta'_1 + \eta'_3 = \eta_1, \quad \eta'_1 \cdot \eta'_3 = -1,$$

indem wir nur an Stelle des Punktes E den Punkt E_1 wählen; wir ziehen also DE_1, welches die Tangente in C im Punkte c'' treffe, und ziehen $c''p$; durch die Schnittpunkte dieser Geraden

mit dem Kreise, welche F_1 und F_3 heissen mögen, ziehen wir CF_1 und CF_3, welche die Tangente in D in den Punkten f_1 und f_3 treffen. Dann ist, da (nach Vorlesung 7) η'_1 positiv, η'_3 negativ ist,

$$Df_1 = \eta'_1, \quad Df_3 = \eta'_3.$$

Jetzt bleiben nur noch die Wurzeln der quadratischen Gleichung (7) zu construiren, d. i. einer derjenigen vier Gleichungen, denen die zweigliedrigen Perioden genügen. Man hat aber

$$\eta''_0 + \eta''_4 = \eta'_0 = Df, \quad \eta''_0 \cdot \eta''_4 = \eta'_1 = Df_1.$$

Vergleichen wir dies mit den allgemeinen Formeln, in welchen wir an Stelle von c und d die Buchstaben c''' und d''', und an Stelle von e und e_1 die Buchstaben h_1 und h_4 setzen wollen, so haben wir

$$Dh_1 + Dh_4 = \frac{4}{Cc'''} = Df, \quad Dh_1 \,.\, Dh_4 = 4 \,.\, \frac{Dd'''}{Cc'''} = Df_1.$$

Hieraus ergiebt sich sogleich die Construction des Punktes c''', da $Cc''' = \frac{4}{Df}$ ist; wir brauchen nur DF zu ziehen, welches die Tangente in C in dem gesuchten Punkte c''' treffen wird. Um d''' zu finden, bemerken wir, dass, wenn $c'''d'''$ den Durchmesser CD in g_1 trifft, das Verhältniss $\frac{Cc'''}{Dd'''}$ ersetzt werden kann durch $\frac{Cg_1}{Dg_1}$, und gleich ist $\frac{4}{Df_1}$; tragen wir daher auf der Tangente in C nach der positiven Seite hin den doppelten Kreisdurchmesser Ck auf und ziehen kf_1, so muss dies den Durchmesser CD in g_1 treffen, und die Verbindungslinie $c'''g_1$ wird den Kreis in solchen zwei Punkten H_1 und H_4 schneiden, dass ihre Verbindungslinien mit C, nämlich CH_1 und CH_4, die Tangente in D in den Punkten h_1 und h_4 treffen, und

$$Dh_1 = \eta''_0 = 2 \cos \frac{2k\pi}{17}, \qquad Dh_4 = \eta''_4 = 2 \cos \frac{2k'\pi}{17}$$

werden, wenn k, k' passend zu wählende ganze Zahlen bezeichnen. Die Linien CH_1 und CH_4 treffen somit den zu den beiden Tangenten in C und D parallelen Kreisdurchmesser AB in zwei Punkten k_1 und k_4, deren Abstände vom Kreismittelpunkte O halb so gross sind, als Dh_1 und Dh_4, es ist also geradezu

$$Ok_1 = \cos \frac{2k\pi}{17}, \qquad Ok_4 = \cos \frac{2k'\pi}{17}.$$

Die Perpendikel in k_1 und k_4, auf dem Durchmesser AB stehend,

werden daher den Kreis in Eckpunkten des gesuchten regulären Siebenzehnecks treffen, dessen erste Ecke A ist.

Die drei ähnlichen quadratischen Gleichungen lassen sich nun in ganz gleicher Weise behandeln, wenn wir nur an Stelle von f und f_1 successive f_1 und f_2, f_2 und f_3, f_3 und f treten lassen. Verfahren wir sonst genau wie zuvor, so erhalten wir auf dem, von C abgewendeten Halbkreise neben den Punkten H_1 und H_4 noch sechs andere, von denen aus man zu allen sechszehn, von A verschiedenen, Ecken des Siebenzehneckes gelangt.

3. Es bleibt jetzt nur noch übrig, die einzelnen Constructionen zu einer möglichst compendiösen Vorschrift für die auszuführende Zeichnung des regulären Siebenzehnecks zusammenzufassen; diese würde folgendermassen lauten*):

In einem Kreise mit dem Radius 1 sind zwei zu einander senkrechte Durchmesser AB, CD gezogen; in C und D werden Tangenten an den Kreis gelegt, auf der Tangente in C nach rechts das Stück Cc, nach links das Stück Ck gleich dem doppelten Kreisdurchmesser abgetragen, auf der Tangente in D wird nach links das Stück DJ gleich dem Radius und ebenfalls nach links das Stück Dd gleich dem doppelten Kreisdurchmesser abgetragen. Sodann zieht man cd, welches den Kreis in E und E_1 trifft, sodass die Punkte d, E, E_1, c auf einander folgen; man zieht DE, DE_1, welche die Tangente in C in ε und ε_1 treffen; ferner möge cJ den Durchmesser CD in p schneiden, dann werden die Verbindungslinien εp und $\varepsilon_1 p$ den Kreis in den Punkten F, F_2 und F_1, F_3, in der Reihenfolge ε, F, p, F_2 und ε_1, F_3, p, F_1 treffen; die vier Strahlen CF, CF_1, CF_2, CF_3 treffen die Tangente in D in den vier Punkten f, f_1, f_2, f_3, die vier Strahlen DF, DF_1, DF_2, DF_3 die Tangente in C in den Punkten φ, φ_1, φ_2, φ_3, die vier Strahlen kf, kf_1, kf_2, kf_3 den Durchmesser CD in den Punkten g, g_1, g_2, g_3. Man ziehe die vier Verbindungslinien φg_1, $\varphi_1 g_2$, $\varphi_2 g_3$, $\varphi_3 g$, welche dem

*) Es erschien nicht nöthig, noch eine besondere Figur dieser Construction beizufügen, da nach den vorhergehenden Betrachtungen es Jedem leicht sein wird, dieselbe selbst herzustellen.

Kreise in den vier Punktpaaren H_1, H_4; H_3, H_5; H_2, H_8; H_6, H_7 begegnen; die acht Strahlen CH_1, CH_2, ... CH_8 treffen den Durchmesser AB in den acht Punkten k_1, k_2, ... k_8, und endlich schneiden die, auf AB in diesen Punkten errichteten Perpendikel den Kreis in 16 Punkten, welche mit dem, nach links liegenden Endpunkte A des Durchmessers die Ecken des, dem Kreise einbeschriebenen Siebenzehnecks bilden.

Diese Construction weicht nur in einigen unwesentlichen Punkten von derjenigen ab, welche v. Staudt im 24. Bande des Crelle'schen Journals pag. 251 ohne Beweis mitgetheilt hat, und von der, wie es scheint, kein Beweis veröffentlicht ist, vielleicht deshalb, weil ein leicht erkennbarer Druckfehler (in der zweiten Zeile statt P zu setzen D) von der Ausführung der Construction abgeschreckt hat. Bei v. Staudt's Auflösung werden bei der zu Grunde liegenden quadratischen Gleichung die reciproken Werthe der Unbekannten eingeführt, was die Gleichungen

$$\frac{1}{De} + \frac{1}{De_1} = \frac{1}{Dd}$$

$$\frac{1}{De} \cdot \frac{1}{De_1} = \frac{Cc}{4Dd}$$

ergiebt, und bei Anwendung dieser Formeln müsste für die Construction der ersten quadratischen Gleichung $Dd = -1$, $Cc = 16$ gesetzt werden, wie es bei v. Staudt der Fall ist; in ähnlicher Weise modificirt sich die Construction der übrigen quadratischen Gleichungen. Die hier mitgetheilte Construction dürfte sich in practischer Beziehung mehr empfehlen, weil sie ein kleineres Operationsfeld beansprucht. (Diese Mittheilung des Hrn. Schröter wird nächstens auch im Crelle'schen Journale erscheinen.)

Achte Vorlesung.

Algebraische Auflösung der Hilfsgleichungen. Die Resolvante und ihre Eigenschaften.

1. In dieser Vorlesung soll gezeigt werden, dass die Hilfsgleichungen, auf welche wir in der 6. Vorlesung die Gleichung $X = 0$ reducirt haben, und welche zur Bestimmung der Perioden

von kleinerer Gliederzahl mittelst der Perioden von grösserer Gliederzahl dienten, ebenso wie die Gleichung $X = 0$ selbst algebraisch auflösbar sind. Verständigen wir uns hiezu vor Allem darüber, was unter algebraischer Auflösung zu verstehen sei.

Man nennt eine Gleichung algebraisch auflösbar, wenn ihre Wurzeln aus den bekannten Grössen gebildet werden können, indem man ausser den rationalen Operationen allein die Operation der Wurzelausziehung benutzt. Der Ausdruck ihrer Wurzeln wird also eine gewisse Anzahl von Radicalen enthalten von der Form $W = \sqrt[n]{T}$, worin T eine rationale Function der bereits bekannten Grössen und daher selbst als bekannt anzusehen ist; W dagegen ist bestimmt als Wurzel einer reinen Gleichung, nämlich der Gleichung $x^n = T$. Hieraus ist ersichtlich, dass die Wurzel einer algebraisch auflösbaren Gleichung bestimmt ist, wenn man eine gewisse Anzahl von reinen Gleichungen aufgelöst hat, oder dass jede algebraisch auflösbare Gleichung auf reine Gleichungen zurückgeführt werden kann. Umgekehrt, wenn es möglich ist, eine Gleichung auf reine Gleichungen zu reduciren, so wird sie algebraisch auflösbar sein.

Nun haben wir gefunden, dass diejenigen e' Perioden, welche eine der f-gliedrigen zusammensetzen, einer Gleichung vom Grade e' genügen, deren Coëfficienten lineare Functionen der f-gliedrigen Perioden sind.

Letztere sollen als bereits gefunden vorausgesetzt und dann soll gezeigt werden, dass jene Gleichung e'^{ten} Grades auf reine Gleichungen desselben Grades zurückgeführt werden kann. Dazu genügt die genauere Untersuchung eines Ausdruckes, auf dessen Wichtigkeit für die Auflösung der Gleichungen zuerst Lagrange aufmerksam gemacht hat*), der sogenannten Resolvante.

Dieselbe hat hier zum Ausdrucke:

$$r + \alpha r^{g^e} + \alpha^2 \,.\, r^{g^{2e}} + \ldots + \alpha^{f-1} \,.\, r^{g^{(f-1)e}},$$

worin α eine Wurzel der Gleichung $x^{e'} = 1$ sein soll, und enthält offenbar nur diejenigen e' Perioden von f' Gliedern, welche die Periode η_0 zusammensetzen, da z. B. die Potenzen

$$r,\; r^{g^{e'e}},\; r^{g^{2e'e}},\; \ldots\; r^{g^{(f'-1)e'e}}$$

*) Lagrange, in den Abhandlungen der Academie zu Berlin, von den Jahren 1770 und 1771, sowie in seinem traité de la résolution des équations numériques.

wegen der Gleichungen:

$$\alpha^{e'} = \alpha^{2e'} = \ldots = \alpha^{(f'-1)e'} = 1$$

denselben Coëfficienten haben. Wir wollen sie mit (α, η'_0) bezeichnen also setzen:

$$(1) \quad (\alpha, \eta'_0) = \eta'_0 + \alpha\eta'_e + \alpha^2 . \eta'_{2e} + \ldots + \alpha^{e'-1} . \eta'_{(e'-1)e}.$$

Ersetzt man hierin r durch r^{g^h}, so gehen die Perioden η'_0, η'_e, η'_{2e}, ... $\eta'_{(e'-1)e}$ in η'_h, η'_{h+e}, η'_{h+2e}, ... $\eta'_{h+(e'-1)e}$ über; der aus (1) hervorgehende Ausdruck kann also passend mit (α, η'_h) bezeichnet werden, da er aus η'_h ebenso entsteht, wie (α, η'_0) aus η'_0. Für $h = e$ findet man so leicht als fundamentale Eigenschaft der Resolvante die Beziehung:

$$(2) \qquad (\alpha, \eta'_e) = \alpha^{-1} . (\alpha, \eta'_0),$$

aus welcher sich allgemeiner für jeden Werth von h:

$$(3) \qquad (\alpha, \eta'_{he}) = \alpha^{-h} . (\alpha, \eta'_0)$$

sowie die Gleichung:

$$(4) \qquad (\alpha, \eta'_{he})^{e'} = (\alpha, \eta'_0)^{e'}$$

d. i. der Umstand ergiebt, dass $(\alpha, \eta'_0)^{e'}$ bei der Substitution von r^{g^e} statt r sich nicht ändert. Nach Nr. 5 der 6. Vorlesung ist also die e'^{te} Potenz der Resolvante eine lineare Function der f-gliedrigen Perioden, deren Coëfficienten ganze und ganzzahlige Functionen von α sind. Wenn man daher annimmt, die Gleichung

$$(5) \qquad x^{e'} = 1$$

sei bereits aufgelöst, sodass α zu den bekannten Grössen zu rechnen ist, ebenso wie die f-gliedrigen Perioden, so wird die e'^{te} Potenz der Resolvante ebenfalls als eine bekannte Grösse anzusehen sein, die wir mit T bezeichnen wollen; die Resolvante selbst dagegen bestimmt sich als eine Wurzel der Gleichung:

$$(6) \qquad x^{e'} = T.$$

Nun scheint es fraglich, welche Wurzel dieser Gleichung man für (α, η'_0) zu wählen hat, indessen überzeugt man sich leicht, dass man eine beliebige dafür annehmen darf, wenn unter α eine primitive Wurzel der Gleichung (5) verstanden wird. In der That sind einerseits die Grössen:

$$(7) \qquad (\alpha, \eta'_0), (\alpha, \eta'_e), \ldots (\alpha, \eta'_{(e'-1)e})$$

sämmtliche Wurzeln der Gleichung (6), denn sie haben erstens

gleiche e'^{te} Potenzen und sind zweitens unter einander verschieden, weil sie sich nach Gleichung (3) wie die, unter einander verschiedenen Potenzen 1, α^{-1}, α^{-2}, . . . $\alpha^{-(e'-1)}$ verhalten. Andererseits ist, sobald die f-gliedrigen Perioden bestimmt sind, r noch insoweit willkürlich, als es eine beliebige der Wurzeln derjenigen Periode bedeutet, welche mit η_0 bezeichnet wird. Ist aber eine derselben r, so sind die übrigen: r^{g^e}, $r^{g^{2e}}$, . . . $r^{g^{(f-1)e}}$, und indem man r^{g^e}, $r^{g^{2e}}$, . . . successive statt r wählt, geht (α, η'_0) successive in (α, η'_e), (α, η'_{2e}), . . . über, sodass man in der That durch passende Wahl von r eine bestimmte Wurzel der Gleichung (6) einer beliebigen der Grössen (7) z. B. also (α, η'_0) gleichmachen kann.

2. Hat man den Ausdruck (α, η'_0) bestimmt, während α eine primitive Wurzel der Gleichung (5) bedeutet, so ergiebt sich der ähnliche Ausdruck (α^n, η'_0) für jeden Werth von n, indem er rational durch jenen ausgedrückt werden kann. Denn ersetzt man einerseits in der Gleichung (2) α durch α^n und erhebt andererseits diese Gleichung in die $(e'-n)^{te}$ Potenz, so findet man die Gleichungen:

$$(2^a) \qquad (\alpha^n, \eta'_e) = \alpha^{-n} \cdot (\alpha^n, \eta'_0)$$
$$(\alpha, \eta'_e)^{e'-n} = \alpha^n \cdot (\alpha, \eta'_0)^{e'-n}$$

und durch deren Multiplication:

$$(8) \qquad (\alpha^n, \eta'_e) \cdot (\alpha, \eta'_e)^{e'-n} = (\alpha^n, \eta'_0) \cdot (\alpha, \eta'_0)^{e'-n}$$

d. h. der Ausdruck $(\alpha^n, \eta'_0) \cdot (\alpha, \eta'_0)^{e'-n}$ hat wieder die Eigenschaft, ungeändert zu bleiben, wenn man r durch r^{g^e} ersetzt, und ist folglich eine lineare Function der f-gliedrigen Perioden mit Coëfficienten, die ganze und ganzzahlige Functionen von α sind. Wird diese, als bekannt zu betrachtende Function durch T_n bezeichnet, so ergiebt sich:

$$(9) \qquad (\alpha^n, \eta'_0) = \frac{T_n}{T} \cdot (\alpha, \eta'_0)^n.$$

Noch findet man, wenn man α durch die Einheit ersetzt, $(1, \eta'_0)$ gleich der Summe derjenigen Perioden, welche die Periode η_0 zusammensetzen, d. i. die Formel

$$(10) \qquad (1, \eta'_0) = \eta_0.$$

Hiernach kann man folgendes System linearer Gleichungen aufstellen:

$$(11)\begin{cases} \eta'_0 + \eta'_e + \eta'_{2e} + \dots + \eta'_{(e'-1)e} = (1, \eta'_0) = \eta_0 \\ \eta'_0 + \alpha\eta'_e + \alpha^2\eta'_{2e} + \dots + \alpha^{e'-1} \cdot \eta'_{(e'-1)e} = (\alpha, \eta'_0) = \sqrt[e']{T} \\ \eta'_0 + \alpha^2\eta'_e + \alpha^4\eta'_{2e} + \dots + \alpha^{2(e'-1)} \cdot \eta'_{(e'-1)e} = (\alpha^2, \eta'_0) = \frac{T_2}{T} \cdot (\sqrt[e']{T})^2 \\ \dots\dots\dots\dots\dots\dots \\ \eta'_0 + \alpha^{e'-1} \cdot \eta'_e + \alpha^{2(e'-1)} \cdot \eta'_{2e} + \dots + \alpha^{(e'-1)(e'-1)}\eta'_{(e'-1)e} \\ \qquad = (\alpha^{e'-1}, \eta'_0) = \frac{T_{e'-1}}{T} \cdot (\sqrt[e']{T})^{e'-1}, \end{cases}$$

deren Auflösung unmittelbar die Perioden η'_0, η'_e, ... $\eta'_{(e'-1)e}$ durch bereits bekannte Grössen ausgedrückt liefert. Es ist nur nöthig, eine derselben, z. B. η'_0 zu bestimmen, da alle übrigen f'-gliedrigen Perioden, wie in Nr. 9 der 6. Vorlesung erwähnt ist, rationale Functionen derselben sind*). Man findet η'_0 durch Addition aller Gleichungen (11), da für jeden der Werthe $h = 1, 2, 3, \dots e' - 1$ die Gleichung

$$1 + \alpha^h + \alpha^{2h} + \dots + \alpha^{(e'-1)h} = 0$$

besteht (s. Vorlesung 3, Gleichung (8)), also die Perioden η'_e, η'_{2e}, ... $\eta'_{(e'-1)e}$ aus der Summe verschwinden. So kommt denn:

$$(12)\ \eta'_0 = \frac{1}{e'}\Big((1, \eta'_0) + (\alpha, \eta'_0) + (\alpha^2, \eta'_0) + \dots + (\alpha^{e'-1}, \eta'_0)\Big)$$
$$= \frac{1}{e'}\left[\eta_0 + \sqrt[e']{T} + \frac{T_2}{T} \cdot (\sqrt[e']{T})^2 + \dots + \frac{T_{e'-1}}{T} \cdot (\sqrt[e']{T})^{e'-1}\right],$$

wo nach Nr. 1 für $\sqrt[e']{T}$ irgend ein Werth dieser e'^{ten} Wurzel genommen werden darf. Da es solcher Werthe genau e' verschiedene giebt, hat der Ausdruck (12) ebensoviele Werthe, welche die e' Perioden $\eta'_0, \eta'_e, \eta'_{2e}, \dots \eta'_{(e'-1)e}$ repräsentiren. Die Formel (12) lehrt, was gezeigt werden sollte, dass die Gleichung vom Grade e', welcher die Periode η'_0 genügt, auf die reinen Gleichungen (5) und (6) desselben Grades zurückführbar ist.

Jedoch bleibt hier ein Einwand zu beseitigen, welcher gegen die Allgemeingültigkeit der soeben gegebenen Methode zur Bestimmung von η'_0 gemacht werden könnte. Geschähe es nämlich, dass T, oder, was dasselbe ist, dass (α, η'_0) gleich Null würde,

---

*) nämlich ohne weitere Auflösung einer Gleichung höheren als des ersten Grades nach der ebds. in Nr. 7 angegebenen Methode gefunden werden können.

so müssten die sämmtlichen Ausdrücke T_n nach Gleichung (8) ebenfalls verschwinden, und deshalb würde die Formel (9) die Ausdrücke (α^n, η'_0) unter einer unbestimmten Form liefern. Es ist also zur Ergänzung des Vorhergehenden nothwendig, nachzuweisen, dass T niemals den Werth Null erhalten kann. Dies ergiebt sich aber als eine einfache Folgerung aus dem in Nr. 7 der 5. Vorlesung bewiesenen Kronecker'schen Satze. Denn, bedeutet

$$F_{e'}(x) = 0 \tag{13}$$

die Gleichung für die primitiven Wurzeln der Gleichung (5), so kann die Gleichung $(\alpha, \eta'_0) = 0$ als eine solche aufgefasst werden, welche eine Wurzel r mit der Kreistheilungsgleichung gemeinsam und ganze und ganzzahlige Functionen einer Wurzel der Gleichung (13) zu Coëfficienten hat. Da hiernach die beiden Gleichungen:

$$(\alpha, \eta'_0) = 0, \quad r^{p-1} + r^{p-2} + \ldots + r + 1 = 0,$$

von denen die erste mittels der zweiten unter den $(p-2)^{ten}$ Grad erniedrigt angenommen werden kann, zugleich bestünden, müssten die beiden Functionen, welche ihre linken Seiten bilden, einen gemeinsamen Theiler haben, dessen Coëfficienten nothwendig rationale und ganzzahlige Functionen von α sein würden. Einen solchen Factor lässt aber die zweite Function nach jenem Satze nicht zu, folglich muss T von Null verschieden sein.

3. Da T im Allgemeinen ein complexer Werth, also von der Form

$$R(\cos\varphi + i\sin\varphi)$$

sein wird, worin R positiv genommen werden darf, so erhalten wir

$$(14)\quad \begin{cases} (\alpha, \eta'_0)^{e'} = R(\cos\varphi + i\sin\varphi) \\ (\alpha, \eta'_0) = \sqrt[e']{R}\,.\left(\cos\dfrac{\varphi + 2h\pi}{e'} + i\sin\dfrac{\varphi + 2h\pi}{e'}\right), \end{cases}$$

in welcher letzten Formel unter $\sqrt[e']{R}$ der positive Werth dieser Wurzel zu verstehen ist. Beachten wir nun, dass α^{-1}, r^{-1} resp. zu α, r die conjugirt imaginären Werthe sind, sowie dass durch die Substitution von r^{-1} d. i. $r^{g^{\frac{p-1}{2}}}$ statt r die Perioden η'_0, η'_e, $\ldots$ $\eta'_{(e'-1)e}$ in $\eta'_{\frac{p-1}{2}}$, $\eta'_{\frac{p-1}{2}+e}$, $\ldots$ $\eta'_{\frac{p-1}{2}+(e'-1)e}$ übergehen,

so wird auch $\left(\alpha^{-1}, \eta'_{\frac{p-1}{2}}\right)$ zu (α, η'_0)conjugirt imaginär sein, und die Gleichung (14) folgende Gleichung:

$$\left(\alpha^{-1}, \eta'_{\frac{p-1}{2}}\right)^{e'} = R\,(\cos\varphi - i\sin\varphi)$$

und, wenn sie mit dieser multiplicirt wird, die nachstehende:

$$(15) \qquad \left[(\alpha, \eta'_0)\,.\left(\alpha^{-1}, \eta'_{\frac{p-1}{2}}\right)\right]^{e'} = R^2$$

liefern. Unter Anwendung der Gleichungen (2) und (2a) aber ergiebt sich

$$(\alpha, \eta'_e)\,.\left(\alpha^{-1}, \eta'_{\frac{p-1}{2}+e}\right) = (\alpha, \eta'_0)\,.\left(\alpha^{-1}, \eta'_{\frac{p-1}{2}}\right)$$

also ist $(\alpha, \eta'_0)\,.\left(\alpha^{-1}, \eta'_{\frac{p-1}{2}}\right)$ wieder ein Ausdruck, der bei der Substitution von r^{g^e} statt r sich nicht ändert, dessen Werth also als eine bekannte Grösse anzusehen ist, welche mit U bezeichnet werde. Hiernach liefert die Gleichung (15) die Beziehung:

$$+\sqrt[e']{R} = +\sqrt[2]{U},$$

wo das Zeichen $+$ andeuten soll, dass auf beiden Seiten der positive Werth der Wurzel zu nehmen ist, und man findet aus (14):

$$(16) \qquad (\alpha, \eta'_0) = +\sqrt{U}\,.\left(\cos\frac{\varphi + 2h\pi}{e'} + i\sin\frac{\varphi + 2h\pi}{e'}\right),$$

während für h irgend eine der Zahlen 0, 1, 2, ... $e'-1$ gewählt werden darf.

Da nun η'_0 vermittelst der Formel (12) rational durch (α, η'_0) und durch bekannte Grössen ausgedrückt worden ist, so ergiebt sich der Satz:

Die Gleichung e'^{ten} Grades, deren Wurzel η'_0 ist, wird aufgelöst, indem man die Gleichung $x^{e'} = 1$ auflöst, einen Winkel, der dann construirt werden kann, in e' gleiche Theile theilt und aus einer bekannten Grösse die Quadratwurzel zieht.

4. Die vorigen Betrachtungen können auch dazu dienen, die Perioden irgend einer Gliederzahl direct zu finden, d. i. ohne erst vorher die Perioden von grösserer Gliederzahl, welche aus ihnen zusammengesetzt sind, bestimmt zu haben. In der That, setzen wir 1, e, f resp. an Stelle von e, e', f', so wird die angegebene Me-

thode uns die *ef*-gliedrigen Perioden durch die Coëfficienten der Kreistheilungsgleichung selbst ausgedrückt liefern. Alles kommt nach dieser Methode darauf an, die Resolvante:

$$(\alpha, \eta_0) = \eta_0 + \alpha\eta_1 + \alpha^2\eta_2 + \ldots + \alpha^{e-1}\eta_{e-1},$$

in welcher α eine primitive Wurzel der Gleichung $x^e = 1$ bedeutet, zu bestimmen. Denn durch ihren Werth können die ähnlichen Functionen (α^2, η_0), (α^3, η_0), ... (α^{e-1}, η_0) nach Formel (9) rational mit Hilfe bekannter Grössen, zu denen die Wurzel α gerechnet wird, ausgedrückt werden, und wenn man (α, η_0) und diese Functionen bestimmt hat, so liefert die Formel (12) sofort für η_0 den Werth:

$$(17) \qquad \eta_0 = \frac{1}{e}\left((1, \eta_0) + (\alpha, \eta_0) + (\alpha^2, \eta_0) + \ldots + (\alpha^{e-1}, \eta_0)\right),$$

in welchem

$$(1, \eta_0) = \eta_0 + \eta_1 + \eta_2 + \ldots + \eta_{e-1} = -1$$

ist. Der Werth von (α, η_0) selbst aber ist als Wurzel einer reinen Gleichung e^{ten} Grades:

$$(18) \qquad x^e = T$$

bestimmt, worin T durch bekannte Grössen, nämlich ausser durch ganze Zahlen allein durch die Wurzel α, rational ausdrückbar ist.

Um nach dieser Methode die Kreistheilungsgleichung selbst direct aufzulösen, muss $e = 1$, $e' = p - 1$, $f' = 1$ angenommen und die Resolvante

$$(19) \qquad (\omega, r) = r + \omega r^g + \omega^2 r^{g^2} + \ldots + \omega^{p-2} \cdot r^{g^{p-2}},$$

in welcher ω eine primitive Wurzel der Gleichung $x^{p-1} = 1$ bedeutet, bestimmt werden. Sie ist aber Wurzel einer reinen Gleichung vom Grade $p - 1$ von der Form:

$$(20) \qquad x^{p-1} = T,$$

wenn unter T eine durch ganze Zahlen und ω rational bekannte Grösse verstanden wird. Ist (ω, r) durch Auflösung dieser Gleichung gefunden, so ergeben sich die Functionen (ω^h, r) für $h = 2, 3, \ldots p-2$ als rationale Functionen von (ω, r) nach Formel (9), und endlich die Wurzel der Kreistheilungsgleichung nach Formel (12) vermittelst folgender Gleichung:

$$(21) \qquad r = \frac{1}{p-1}\left((1, r) + (\omega, r) + (\omega^2, r) + \ldots (\omega^{p-2}, r)\right).$$

Für diesen Fall geht der letzte Satz der Nr. 3 in den folgenden über:

Um die Kreistheilungsgleichung aufzulösen, hat man nur nöthig, die Gleichung $x^{p-1} = 1$ aufzulösen, einen Winkel, welcher dann construirt werden kann, in $p-1$ gleiche Theile zu theilen, und aus einer bekannten Grösse die Quadratwurzel zu ziehen. Diese Grösse ist p, wie nachher gezeigt werden soll.

Wenn man h in dem Ausdrucke (ω^h, r) die Reihe f, $2f$, $3f$, ... $(e-1)f$ durchlaufen lässt und bemerkt, dass ω^f eine primitive Wurzel der Gleichung $x^e = 1$ ist, welche an Stelle von α genommen werden kann, so nimmt der Ausdruck (ω^h, r) successive die Werthe (α, η_0), (α^2, η_0), ... (α^{e-1}, η_0) an. Man hat also offenbar allein den Werth von (ω, r) zu bestimmen, um alle Elemente zu erhalten, welche zur Auflösung der Kreistheilungsgleichung sowie der Periodengleichungen, d. i. derjenigen ganzzahligen Gleichungen, welche die Perioden direct finden lehren, ausser den bekannten Grössen nothwendig sind.

Alles kommt daher darauf an, die Berechnung des Werthes von (ω, r) zu ermöglichen, und zu diesem Zwecke für den hier vorliegenden Fall: $n = 1$, $e' = p-1$, $f' = 1$ die Zusammensetzung der mit T und T_n bezeichneten Ausdrücke näher zu untersuchen.

5. Hierzu führen die folgenden Betrachtungen.

Mit Anwendung des Summenzeichens kann man schreiben:

$$(\omega^h, r) = \sum_{\lambda=0}^{\lambda=p-2} \omega^{h\lambda} \, . \, r^{g^\lambda}. \tag{22}$$

Wenn aber μ den kleinsten positiven Rest von g^λ (mod. p) bedeutet, so ist $\lambda = \text{ind.}\,\mu$ und die in $r^{g^\lambda} = r^\mu$ multiplicirte Potenz von ω gleich $\omega^{h\,\text{ind.}\,\mu}$; ferner erhält μ die ganzzahligen Werthe $1, 2, 3, \ldots . p-1$, wenn λ die Werthe $0, 1, 2, \ldots . p-2$ durchläuft. Indem man also nach steigenden Potenzen von r ordnet, kann man auch schreiben:

$$(\omega^h, r) = \sum_{\mu=1}^{\mu=p-1} \omega^{h\,\text{ind.}\,\mu} \, . \, r^\mu. \tag{22a}$$

Für $h = 0$ liefert diese Formel:

$$(1, r) = r + r^2 + \ldots . + r^{p-1} = -1. \tag{23}$$

Wendet man die Gleichung (2a) auf den vorliegenden Fall an, so wird die fundamentale Eigenschaft der Resolvante (ω, r) durch folgende Gleichung:

$$(24)\qquad (\omega^h, r^g) = \omega^{-h} \, . \, (\omega^h, r)$$

ausgedrückt, aus welcher sich, wenn $h = f$, also $\omega^f = \alpha$ eine Wurzel der Gleichung $x^e = 1$ und $(\omega^f, r) = (\alpha, \eta_0)$ ist, durch Erhebung zur e^{ten} Potenz die Gleichung:

$$(\omega^f, r^g)^e = (\omega^f, r)^e$$

oder:

$$(25)\qquad (\alpha, \eta_1)^e = (\alpha, \eta_0)^e,$$

also, in Uebereinstimmung mit der im Vorigen entwickelten Theorie, schon $(\alpha, \eta_0)^e$ als eine bei der Substitution von r^g statt r unveränderliche und deshalb durch die bekannten Grössen ausdrückbare Function ergiebt; während, wenn $h = 1$ gesetzt wird, aus (24) erst

$$(26)\qquad (\omega, r^g)^{p-1} = (\omega, r)^{p-1},$$

d. i. erst die $(p-1)^{te}$ Potenz der Resolvante rational bekannt wird.

Um aber diese Potenzen und damit die reinen Gleichungen, von welchen die Resolvanten abhängen, wirklich zu bestimmen, wollen wir das Product

$$(\omega^h, r) \, . \, (\omega^k, r)$$

entwickeln, indem wir unter h, k zwei solche ganze Zahlen verstehen, deren Summe durch $p-1$ nicht theilbar ist. Nach Formel (22a) wird man dies Product als eine Doppelsumme schreiben können, wie folgt:

$$(\omega^h, r) \, . \, (\omega^k, r) = \sum_{\mu'=1}^{\mu'=p-1} \sum_{\mu=1}^{\mu=p-1} \omega^{h \operatorname{ind}.\mu + k \operatorname{ind}.\mu'} \, . \, r^{\mu+\mu'}.$$

In derselben bilden diejenigen Glieder, welchen derselbe Werth von μ' zukommt, die einfache Summe:

$$\sum_{\mu=1}^{\mu=p-1} r^{\mu+\mu'} \, . \, \omega^{h \operatorname{ind}.\mu + k \operatorname{ind}.\mu'}.$$

Da nun, wenn μ alle ganzen Zahlen $1, 2, 3, \ldots . p-1$ durchläuft, gleichzeitig das Product $\mu\mu'$ diesen Zahlen, wenn auch in anderer Ordnung, (mod. p) congruent wird, da ferner einander (mod. p) congruente Zahlen im Exponenten von r für einander gesetzt werden dürfen, und die Indices solcher Zahlen einander

gleich sind, so kann man offenbar den Summationsbuchstaben μ durch $\mu\mu'$ ersetzen, wodurch, mit Benutzung der Relation (s. 4. Vorlesung Nr. 10, 1)):

$$\text{ind.}\,\mu\mu' \equiv \text{ind.}\,\mu + \text{ind.}\,\mu' \mod (p-1)$$

jene einfache Summe die Gestalt:

$$\sum_{\mu=1}^{\mu=p-1} \omega^{h\,\text{ind.}\,\mu+(h+k)\,\text{ind.}\,\mu'} \,.\, r^{(1+\mu)\mu'}$$

annimmt. Dann ergiebt sich zunächst:

$$(\omega^h, r)\,.\,(\omega^k, r) = \sum_{\mu'=1}^{\mu'=p-1}\sum_{\mu=1}^{\mu=p-1} \omega^{h\,\text{ind.}\,\mu+(h+k)\,\text{ind.}\,\mu'} \,.\, r^{(1+\mu)\mu'}.$$

Beginnt man nun mit der Summation, welche sich auf μ' bezieht, so ist die einfache Summe:

$$\sum_{\mu'=1}^{\mu'=p-1} \omega^{(h+k)\,\text{ind.}\,\mu'} \,.\, r^{(1+\mu)\mu'}$$

zu bilden, wofür man aus Formel (22a), wenn man darin $r^{1+\mu}$ statt r und $h+k$ statt h setzt, folgende Gleichung findet:

$$(27)\qquad \sum_{\mu'=1}^{\mu'=p-1} \omega^{(h+k)\,\text{ind.}\,\mu'} \,.\, r^{(1+\mu)\mu'} = (\omega^{h+k}, r^{1+\mu}).$$

Unter den Werthen, welche μ erhalten soll, ist nur einer, nämlich $\mu=p-1$, für welchen $1+\mu$ durch p theilbar ist; diesem entsprechend wird der Werth der einfachen Summe gleich

$$(\omega^{h+k}, 1) = 1 + \omega^{h+k} + \omega^{2(h+k)} + \ldots + \omega^{(p-2)(h+k)},$$

d. i. (nach 3. Vorlesung, Gleichung (8)) gleich Null, da $h+k$ nicht durch $p-1$ theilbar ist. Für die übrigen Werthe von μ ist, da sich durch wiederholte Anwendung der Gleichung (24):

$$(\omega^h, r^{g^m}) = \omega^{-hm}\,.\,(\omega^h, r)$$

oder auch:

$$(24\text{a})\qquad (\omega^h, r^n) = \omega^{-h\,\text{ind.}\,n}\,.\,(\omega^h, r)$$

ergiebt,

$$(\omega^{h+k}, r^{1+\mu}) = \omega^{-(h+k)\,\text{ind.}\,(1+\mu)}\,.\,(\omega^{h+k}, r).$$

Wird dieser Werth in die Gleichung (27) substituirt, so kommt:

$$\sum_{\mu'=1}^{\mu'=p-1} \omega^{(h+k)\,\text{ind.}\,\mu'} \,.\, r^{(1+\mu)\mu'} = \omega^{-(h+k)\,\text{ind.}\,(1+\mu)}\,.\,(\omega^{h+k}, r),$$

wo der zweite Factor vom Summationsbuchstaben μ völlig unab-

hängig ist, also bei der nun auszuführenden Summation nach μ als gemeinsamer Factor heraustritt, sodass man endlich findet:

$$(28) \qquad \frac{(\omega^h, r) \cdot (\omega^k, r)}{(\omega^{h+k}, r)} = \sum_{\mu=1}^{\mu=p-2} \omega^{h\,\text{ind.}\mu - (h+k)\,\text{ind.}\,(1+\mu)}.$$

Der Quotient auf der linken Seite ist also eine ganze und ganzzahlige Function der Wurzel ω oder, wie man zu sagen pflegt, eine aus der Wurzel ω gebildete complexe ganze Zahl.

Aus der Symmetrie des Quotienten in Bezug auf h und k folgt, dass die Summe auf der rechten Seite auch durch die andere:

$$\sum_{\nu=1}^{\nu=p-2} \omega^{k\,\text{ind.}\nu - (h+k)\,\text{ind.}\,(1+\nu)}$$

ersetzt werden kann, wovon man sich auch leicht folgendermassen überzeugt. Man bestimme ν als die positive Zahl, welche kleiner als p ist und der Congruenz $\mu\nu \equiv 1$ (mod. p) genügt, so werden μ, ν gleichzeitig, wenn auch in verschiedener Reihenfolge, die Reihe der ganzen Zahlen 1, 2, 3, ... $p-2$ durchlaufen, denn für die Werthe von μ aus dieser Reihe erhält ν verschiedene Werthe der Reihe 1, 2, 3, ... $p-1$ mit Ausschluss des letzten, welcher dem Werthe $\mu = p-1$ entsprechen würde, und umgekehrt. Da nun

$$\begin{gathered} \text{ind.}\,\mu \equiv -\,\text{ind.}\,\nu \quad \text{mod. } (p-1) \\ \text{ind.}\,(1+\mu) + \text{ind.}\,\nu \equiv \text{ind.}\,(\nu+\mu\nu) \equiv \text{ind.}\,(\nu+1), \\ \text{also ind.}\,(1+\mu) \equiv -\,\text{ind.}\,\nu + \text{ind.}\,(1+\nu) \end{gathered}$$

ist, so ergiebt sich

$$h\,\text{ind.}\mu - (h+k)\,\text{ind.}\,(1+\mu) \equiv k\,\text{ind.}\nu - (h+k)\,\text{ind.}\,(1+\nu)\ \text{mod.}\,(p-1)$$

und folglich die Gleichheit der beiden Summen.

6. Die Formel (28) verliert ihre Gültigkeit, wenn $k = -h$ gesetzt wird, da dann die Summe $h + k$ gleich Null, also durch $p - 1$ theilbar würde. Bildet man aber direct das Product $(\omega^h, r) \cdot (\omega^{-h}, r)$, so findet man es als Doppelsumme:

$$(\omega^h, r) \cdot (\omega^{-h}, r) = \sum_{\mu=1}^{\mu=p-1} \sum_{\mu'=1}^{\mu'=p-1} \omega^{h(\text{ind.}\mu - \text{ind.}\mu')} \cdot r^{\mu+\mu'}.$$

Wenn man nun ganz so verfährt, wie in dem allgemeinen Falle, indem man für jeden stehenden Werth von μ' an Stelle

von μ schreibt $\mu\mu'$ und darauf zuerst in Bezug auf μ' summirt, so erhält man:

$$(\omega^h, r) \cdot (\omega^{-h}, r) = \sum_{\mu=1}^{\mu=p-1} \sum_{\mu'=1}^{\mu'=p-1} \omega^{h \operatorname{ind.} \mu} \cdot r^{\mu'(1+\mu)}$$

$$= \sum_{\mu=1}^{\mu=p-1} \omega^{h \operatorname{ind.} \mu} \left(r^{1+\mu} + r^{2(1+\mu)} + \ldots + r^{(p-1)(1+\mu)}\right).$$

So oft $1+\mu$ von p verschieden ist, hat die Summe in der Klammer den Werth -1, nur für den einzigen Werth $\mu = p-1$ ist sie gleich $p-1$, folglich findet man:

$$(\omega^h, r) \cdot (\omega^{-h}, r) = p \cdot \omega^{h \operatorname{ind.} (p-1)} - \sum_{\mu=1}^{\mu=p-1} \omega^{h \operatorname{ind.} \mu}.$$

Nun ist ind. $(p-1) = \frac{p-1}{2}$, und aus

$$\omega^{p-1} - 1 = \left(\omega^{\frac{p-1}{2}} + 1\right)\left(\omega^{\frac{p-1}{2}} - 1\right) = 0$$

folgt $\omega^{\frac{p-1}{2}} = -1$, da sonst ω nicht eine primitive $(p-1)^{te}$ Einheitswurzel sein würde. Ist ferner h durch $p-1$ nicht theilbar, so ist die Summe offenbar gleich

$$1 + \omega^h + \omega^{2h} + \ldots + \omega^{(p-2)h} = \frac{\omega^{(p-1)h} - 1}{\omega^h - 1} = 0,$$

weil, indem μ die Reihe $1, 2, 3, \ldots p-1$, ind. μ die Reihe $0, 1, 2, \ldots p-2$ durchläuft. Man findet also, sobald h durch $p-1$ nicht theilbar ist, die Gleichung:

$$(29) \qquad (\omega^h, r) \cdot (\omega^{-h}, r) = (-1)^h \cdot p.$$

Später werden wir auf diese wichtige Formel mehrfach zurückzukommen Gelegenheit haben; hier wollen wir sie nur benutzen, um durch Verbindung mit der Formel (24a) dem in Nr. 4 gegebenen Versprechen zu genügen. Ersetzt man in (29) die Wurzel r durch r^{-1}, multiplicirt die entstehende Gleichung mit (29) und setzt $h=1$, so ergiebt sich:

$$(\omega, r) \cdot (\omega^{-1}, r^{-1}) \cdot (\omega^{-1}, r) \cdot (\omega, r^{-1}) = p^2.$$

Hierin sind aber die beiden Factoren $(\omega, r) \cdot (\omega^{-1}, r^{-1})$ und $(\omega^{-1}, r) \cdot (\omega, r^{-1})$ einander gleich, wie leicht aus (24a) abzuleiten ist, und als Producte zweier offenbar conjugirt imaginärer Grössen auch positiv. Zieht man also aus beiden Seiten der vorhergehenden Gleichung die Quadratwurzel aus, so ergiebt sich:

$$(\omega, r) \cdot (\omega^{-1}, r^{-1}) = p;$$

das Product $(\omega, r) \cdot (\omega^{-1}, r^{-1})$ tritt aber genau an die Stelle der Grösse U, wenn die in Nr. 2 auseinandergesetzte Methode auf den Fall $e = 1, e' = p - 1, f' = 1$, d. i. zur Auflösung der Kreistheilungsgleichung selbst angewendet wird.

7. Die Formeln (28) und (29) führen nun zu einer andern sehr wichtigen Formel, welche uns alle Elemente liefern wird, deren man zur Auflösung der Kreistheilungs- und Periodengleichungen bedarf.

Nehmen wir $k = nh$, so wird die Summe auf der rechten Seite der Gleichung (28) eine ganze und ganzzahlige Function von ω^h oder, wie wir sagen wollen, eine aus ω^h gebildete complexe ganze Zahl, die mit $\psi_n(\omega^h)$ bezeichnet werden mag, sodass jene Gleichung die Form annimmt:

$$(30) \qquad (\omega^h, r) \cdot (\omega^{nh}, r) = (\omega^{(n+1)h}, r) \cdot \psi_n(\omega^h),$$

worin wir voraussetzen, dass keine der drei Zahlen $h, nh, (n+1)h$ durch $p - 1$ theilbar ist. Bildet man diese Gleichung für $n = 1, 2, 3 \ldots . m - 1$, multiplicirt alle entstehenden Gleichungen in einander und hebt die gleichen Factoren aus beiden Seiten heraus, so ergiebt sich die erwähnte Formel:

$$(31) \qquad (\omega^h, r)^m = (\omega^{mh}, r) \cdot \psi_1(\omega^h) \cdot \psi_2(\omega^h) \ldots . \psi_{m-1}(\omega^h).$$

Setzt man nun $h = 1$, so darf man in der Gleichung (30) für n alle ganze Zahlen $1, 2, 3, \ldots . p - 3$ wählen, ohne dass eine der Zahlen $h, nh, (n+1)h$ durch $p - 1$ theilbar würde; also geht aus der vorhergehenden Fundamentalgleichung die folgende hervor:

$$(32) \qquad (\omega, r)^m = (\omega^m, r) \cdot \psi_1(\omega) \, \psi_2(\omega) \ldots . \psi_{m-1}(\omega),$$

welche für alle m, die kleiner als $p - 1$ sind, den Werth des Ausdrucks (ω^m, r) rational durch (ω, r) und bekannte Grössen ausgedrückt liefert.

Um die reine Gleichung zu finden, durch welche (ω, r) selbst bestimmt wird, setze man $m = p - 2$, und verbinde die so aus (32) entstehende Gleichung:

$$(\omega, r)^{p-2} = (\omega^{p-2}, r) \cdot \psi_1(\omega) \cdot \psi_2(\omega) \ldots . \psi_{p-3}(\omega)$$

durch Multiplication mit der Gleichung:

$$(\omega, r) \cdot (\omega^{p-2}, r) = -p,$$

welche für $h = 1$ aus (29) sich ergiebt, so entsteht die gesuchte Gleichung:

(33) $$(\omega, r)^{p-1} = -p \cdot \psi_1(\omega)\,\psi_2(\omega) \ldots \psi_{p-3}(\omega),$$

auf deren Auflösung alles Andere zurückkommt.

Nun ist zwar in Nr. 4 bemerkt worden, dass (α, η_0) und die ähnlichen Functionen durch (ω, r) und bekannte Grössen ausgedrückt werden können, und zwar geschieht dies ebenfalls mit Hilfe der Formel (32), wenn statt m die Werthe $f, 2f, \ldots (e-1)f$ genommen werden. Indessen mag gezeigt werden, wie die Gleichung (31) dazu benutzt werden kann, auch die reine Gleichung (18) zu bestimmen, aus deren Auflösung die Function (α, η_0) direct erhalten wird. Setzt man $h = f$ und $\omega^f = \alpha$, so wird $(\omega^f, r) = (\alpha, \eta_0)$. Die Formel (30) darf in diesem Falle angewendet werden, so lange keine der Zahlen nf, $(n+1)f$ durch $p-1$, folglich keine der Zahlen n, $n+1$ durch e theilbar ist; indem man also n die Werthe 1, 2, 3, ... $e-2$ durchlaufen lässt und mit der aus (31) sich ergebenden Gleichung:

$$(\alpha, \eta_0)^{e-1} = (\alpha^{e-1}, \eta_0) \cdot \psi_1(\alpha)\,\psi_2(\alpha) \ldots \psi_{e-2}(\alpha)$$

die folgende:

$$(\alpha, \eta_0) \cdot (\alpha^{e-1}, \eta_0) = (-1)^f \cdot p$$

verbindet, welche unter denselben Voraussetzungen aus der Gleichung (29) entspringt, findet man:

(34) $$(\alpha, \eta_0)^e = (-1)^f \cdot p \cdot \psi_1(\alpha)\,\psi_2(\alpha) \ldots \psi_{e-2}(\alpha).$$

Endlich giebt die Formel (31) unter denselben Voraussetzungen für alle Werthe von m, welche kleiner als e sind, die Gleichung:

(35) $$(\alpha, \eta_0)^m = (\alpha^m, \eta_0) \cdot \psi_1(\alpha)\,\psi_2(\alpha) \ldots \psi_{m-1}(\alpha),$$

um direct durch (α, η_0) die ähnlichen Functionen (α^2, η_0), (α^3, η_0), ... (α^{e-1}, η_0) auszudrücken.

Setzt man für die rechte Seite der Gleichung (33) zur Abkürzung wieder T, und zerlegt den Bruch $\frac{1}{p-1}$ nach Gauss' Disqu. arithm. art. 310 in Partialbrüche:

$$\frac{1}{p-1} = \frac{m}{q^a} + \frac{m_1}{q_1^{a_1}} + \ldots \pm n,$$

worin q^a, $q_1^{a_1}$, ... die verschiedenen, in $p-1$ enthaltenen

Primzahlpotenzen, $n, m, m_1, \ldots$ positive ganze Zahlen bedeuten, von denen $m < q^a$, $m_1 < q_1^{a_1}, \ldots$ ist, so kann man setzen:

$$(36) \qquad (\omega, r) = T^{\pm n} . \sqrt[q^a]{T^m} . \sqrt[q_1^{a_1}]{T^{m_1}} \ldots,$$

und zwar darf bei jedem der hier auftretenden Wurzelzeichen nach Belieben einer der möglichen Werthe gewählt werden, da ihre Combination im Ganzen die $p-1$ verschiedenen Werthe von $\sqrt[p-1]{T}$ ergiebt, unter welchen ein beliebiger nach Ende von Nr. 1 für (ω, r) angenommen werden darf.

Weil nun alle Elemente der Auflösung, soweit sie nicht bereits zu den bekannten Grössen gerechnet werden, rational durch (ω, r) ausdrückbar gefunden worden sind, so werden ausser den Wurzelzeichen der Grade q^a, $q_1^{a_1}, \ldots$, welche der Ausdruck (36) enthält, nirgends andere auftreten, als die bereits bekannten Grössen in sich enthalten. Diese sind aber ausser den ganzen Zahlen nur gewisse Einheitswurzeln. Deshalb werden überall nur solche Wurzelzeichen vorkommen können, welche Primzahlpotenzen zu Exponenten haben, indem auch jene Einheitswurzeln nach Nr. 6 der 3. Vorlesung durch solche von Primzahlpotenzgraden ausgedrückt werden können.

8. Wenn es theoretisch am Einfachsten ist, alle Resolvanten durch die einzige (ω, r) auszudrücken, und diese allein durch Auflösung einer reinen Gleichung zu bestimmen, so ist es doch, wenn man die Auflösung der Kreistheilungsgleichung auf die einfachsten Elemente zurückführen und dadurch, ausser einer weiteren Einsicht in die Natur der Einheitswurzeln, leichtere Ausführbarkeit der Rechnungen gewinnen will, vorzuziehen, einen umgekehrten Weg zu verfolgen. In Jacobi's Vorlesungen über Zahlentheorie findet sich eine grössere Reihe dahin zielender Untersuchungen, deren Hauptresultate er auch in seiner Note: „über die Kreistheilung und ihre Anwendung auf die Zahlentheorie*)“ mitgetheilt hat. Es mag hier genügen, eins derselben zu beweisen, welches sich in dem Satze aussprechen lässt: Um alle Resolvanten (ω^m, r) zu bestimmen, reicht es hin, diejenigen zu finden, bei welchen ω^m eine primitive Einheitswurzel von einem Primzahlpotenzgrade ist. Setzen wir, um dies zu erkennen, $p-1 = q^a . q_1^{a_1} \ldots q_i^{a_i}$ voraus und

*) In Crelle's J. Bd. 30.

$$\varphi = \frac{p-1}{q^a}, \quad \varphi_1 = \frac{p-1}{q_1^{a_1}}, \ldots \varphi_i = \frac{p-1}{q_i^{a_i}};$$

bedeutet dann m irgend eine ganze Zahl, welche kleiner als $p-1$ ist, so kann man bekanntlich*)

(37) $$m = n.\varphi + n_1\varphi_1 + \ldots + n_i\varphi_i + z(p-1)$$

setzen, während $n, n_1, \ldots n_i$ positive Zahlen bedeuten, welche resp. kleiner sind als $q^a, q_1^{a_1}, \ldots q_i^{a_i}$, z aber eine positive oder negative ganze Zahl. Daraus folgt zunächst, da $\omega^{p-1} = 1$ ist,

(38) $$(\omega^m, r) = (\omega^{n\varphi+n_1\varphi_1+\ldots+n_i\varphi_i}, r).$$

Bezeichnen wir nun mit $\psi(h, k, \omega)$ den Ausdruck $\frac{(\omega^h, r).(\omega^k, r)}{(\omega^{h+k}, r)}$, welcher nach (28) eine ganze und ganzzahlige Function allein von ω ist, wenn $h+k$ durch $p-1$ nicht theilbar ist, so werden sich successive folgende Gleichungen:

$$(\omega^{n\varphi}, r).(\omega^{n_1\varphi_1}, r) = \psi(n\varphi, n_1\varphi_1, \omega).(\omega^{n\varphi+n_1\varphi_1}, r)$$

$$(\omega^{n\varphi+n_1\varphi_1}, r).(\omega^{n_2\varphi_2}, r) = \psi(n\varphi+n_1\varphi_1, n_2\varphi_2, \omega).(\omega^{n\varphi+n_1\varphi_1+n_2\varphi_2}, r)$$

. . . .

$$(\omega^{n\varphi+\ldots+n_{i-1}\varphi_{i-1}}, r).(\omega^{n_i\varphi_i}, r)$$
$$= \psi(n\varphi+\ldots+n_{i-1}\varphi_{i-1}, n_i\varphi_i, r).(\omega^{n\varphi+\ldots+n_i\varphi_i}, r)$$

aufstellen lassen, aus deren Multiplication man mit Rücksicht auf (38)

(39) $$(\omega^m, r) = \frac{(\omega^{n\varphi}, r).(\omega^{n_1\varphi_1}, r)\ldots(\omega^{n_i\varphi_i}, r)}{\Psi(\omega)}$$

findet, wenn unter $\Psi(\omega)$ das Product

$$\psi(n\varphi, n_1\varphi_1, \omega)\,\psi(n\varphi+n_1\varphi_1, n_2\varphi_2, \omega)\ldots\psi(n\varphi+\ldots+n_{i-1}\varphi_{i-1}, n_i\varphi_i, \omega)$$

verstanden wird, welches eine gewisse ganze und ganzzahlige Function von ω allein sein muss, da die Summe der beiden ganzen Zahlen, welche in den einzelnen ψ-Functionen auftreten, wie leicht zu sehen ist, niemals durch $p-1$ theilbar sein kann.

Es sei nun $\delta = q^{a-\alpha}.q_1^{a_1-\alpha_1}\ldots q_i^{a_i-\alpha_i}$ der grösste gemeinsame Theiler von m und $p-1$, so dass nach Nr. 4 der 3. Vorlesung ω^m eine primitive Einheitswurzel des Grades $q^\alpha q_1^{\alpha_1}\ldots q_i^{\alpha_i}$ ist, so lehrt die Gleichung (37), da $\varphi_1, \varphi_2 \ldots \varphi_i$ sämmtlich durch q^a theilbar sind, dass die grösste den Zahlen n und $p-1$ gemeinsame Potenz von q gleich $q^{a-\alpha}$, der grösste gemeinsame Theiler der Zahlen $n\varphi$ und $p-1$ gleich $q^{a-\alpha}.q_1^{a_1}\ldots q_i^{a_i}$ sein wird, folglich ist $\omega^{n\varphi}$ eine primitive Einheitswurzel des Prim-

*) Vergl. Gauss Disqu. art. 310.

zahlpotenzgrades q^a. Ebenso ergeben sich $\omega^{n_1 \varphi_1}, \ldots \omega^{n_i \varphi_i}$ als primitive Einheitswurzeln von den Primzahlpotenzgraden $q_1^{a_1}, \ldots q_i^{a_i}$ resp., womit nach Gleichung (39) der behauptete Satz als richtig dargethan ist.

Diejenigen Resolvanten (ω^h, r) aber, bei welchen ω^h eine Einheitswurzel vom Grade q^a ist, können folgendermassen gefunden werden: Setzt man in Formel (31) $m = q$, so geht durch Ausziehen einer q^{ten} Wurzel die Gleichung:

$$(40) \quad (\omega^h, r) = \sqrt[q]{\psi_1(\omega^h) \cdot \psi_2(\omega^h) \ldots \psi_{q-1}(\omega^h) \cdot (\omega^{hq}, r)},$$

und, wenn man hierin ω durch $\omega^q, \omega^{q^2}, \ldots \omega^{q^{a-2}}$ ersetzt, die folgenden:

$$(41) \begin{cases} (\omega^{hq}, r) = \sqrt[q]{\psi_1(\omega^{hq}) \cdot \psi_2(\omega^{hq}) \ldots \psi_{q-1}(\omega^{hq}) \cdot (\omega^{hq^2}, r)} \\ (\omega^{hq^2}, r) = \sqrt[q]{\psi_1(\omega^{hq^2}) \cdot \psi_2(\omega^{hq^2}) \ldots \psi_{q-1}(\omega^{hq^2}) \cdot (\omega^{hq^3}, r)} \\ \ldots \\ (\omega^{hq^{a-2}}, r) = \sqrt[q]{\psi_1(\omega^{hq^{a-2}}) \ldots \psi_{q-1}(\omega^{hq^{a-2}}) \cdot (\omega^{hq^{a-1}}, r)} \end{cases}$$

hervor. Wenn man ferner in Gleichung (31) ω durch $\omega^{q^{a-1}}$, m durch $q-1$ ersetzt und mit $(\omega^{hq^{a-1}}, r)$ multiplicirt, so findet man, da

$$\omega^{(q-1)hq^{a-1}} = \omega^{hq^a} \cdot \omega^{-hq^{a-1}} \text{ und } (\omega^h)^{q^a} = 1 \text{ ist,}$$

$$(\omega^{hq^{a-1}}, r)^q = \psi_1(\omega^{hq^{a-1}}) \ldots \psi_{q-2}(\omega^{hq^{a-1}}) \cdot (\omega^{hq^{a-1}}, r) \cdot (\omega^{-hq^{a-1}}, r).$$

Nun ist nach (29):

$$(\omega^{hq^{a-1}}, r) \cdot (\omega^{-hq^{a-1}}, r) = (-1)^{hq^{a-1}} \cdot p,$$

folglich ergiebt sich eine letzte Formel:

$$(42) \quad (\omega^{hq^{a-1}}, r) = \sqrt[q]{\psi_1(\omega^{hq^{a-1}}) \ldots \psi_{q-2}(\omega^{hq^{a-1}}) \cdot (-1)^{hq^{a-1}} \cdot p}$$

welche, mit den Formeln (40) und (41) verbunden, durch a auf einander folgende Wurzelausziehungen vom Grade q den Ausdruck (ω^h, r) finden lehrt.

Die $q-1$ ψ-Functionen, welche in diesen Formeln auftreten, können sogar auf eine noch geringere Anzahl reducirt und die Rechnung dadurch vereinfacht werden. Indessen scheint es mir nicht angezeigt, diese feineren Untersuchungen Jacobi's hier zu reproduciren.*)

---

*) S. übrigens auch in Gauss op. Bd. II. disquisitionum circa aequationes puras ulterior evolutio, art. 16.

9. Dagegen müssen wir noch darauf eingehen, zu zeigen, wie die aus ω^h gebildeten complexen ganzen Zahlen $\psi_n(\omega^h)$ in jedem Falle nach einem gleichbleibenden Algorithmus gebildet werden können. Ist ω^h eine primitive Wurzel der Gleichung $x^e = 1$, was z. B. der Fall sein wird, wenn $h = f$ und $p - 1 = e \,.\, f$ angenommen wird, so erhält man, indem man $\omega^h = \alpha$ setzt:

$$\psi_n(\alpha) = \sum_{\mu=1}^{\mu=p-2} \alpha^{\text{ind.}\,\mu - (n+1)\,\text{ind.}\,(1+\mu)}.$$

Da in dieser Summe für die Exponenten von α ihre Reste (mod. e) gesetzt werden dürfen, so braucht man nur für irgend eine primitive Wurzel g vom Modulus p die Indices von μ und $1+\mu$ für die Werthe $\mu = 1, 2, 3 \ldots . p-2$ aufzustellen, ind. $\mu - (n+1)$ ind. $(1+\mu)$ zu berechnen, und einfach abzuzählen, wie oft unter den Resten von ind. $\mu - (n+1)$ ind. $(1+\mu)$ (mod. e) sich die Zahlen $0, 1, 2, \ldots . e-1$ befinden; nennt man diese Mengen resp. $A_0, A_1, \ldots . A_{e-1}$, so dass

(43) $$A_0 + A_1 + A_2 + \ldots . + A_{e-1} = p - 2$$

ist, so ergiebt sich:

(44) $$\psi_n(\alpha) = A_0 + A_1\alpha + A_2\alpha^2 + \ldots . + A_{e-1}\alpha^{e-1}.$$

Sei z. B. $p = 61$ und $\psi_1(\alpha)$ zu berechnen, wo α eine primitive Wurzel der Gleichung $x^5 = 1$, also $e = 5$ ist. Man kann $g = 2$ nehmen und erhält dann folgendes Schema zur Berechnung der complexen Zahl

$$\psi_1(\alpha) = \sum_{\mu=1}^{\mu=59} \alpha^{\text{ind.}\,\mu - 2\,\text{ind.}\,(1+\mu)}:$$

$\mu =$	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,	13,	14,	15,	16,	17,	18,	19,	20,
ind. $\mu =$	0,	1,	6,	2,	22,	7,	49,	3,	12,	23,	15,	8,	40,	50,	28,	4,	47,	13,	26,	24,
ind. $\mu - 2$. ind. $(1+\mu) \equiv$ (mod. 5)	3,	4,	2,	3,	3,	4,	3,	4,	1,	3,	4,	3,	0,	4,	0,	0,	1,	1,	3,	4,

$\mu =$	21,	22,	23,	24,	25,	26,	27,	28,	29,	30,	31,	32,	33,	34,	35,	36,	37,	38,	39,	40,
ind. $\mu =$	55,	16,	57,	9,	44,	41,	18,	51,	35,	29,	59,	5,	21,	48,	11,	14,	39,	27,	46,	25,
ind. $\mu - 2$. ind. $(1+\mu) \equiv$ (mod. 5)	3,	2,	4,	1,	2,	0,	1,	1,	2,	1,	4,	3,	0,	1,	3,	1,	0,	0,	1,	2,

$\mu =$	41,	42,	43,	44,	45,	46,	47,	48,	49,	50,	51,	52,	53,	54,	55,	56,	57,	58,	59,	60.
ind. $\mu =$	54,	56,	43,	17,	34,	58,	20,	10,	38,	45,	53,	42,	33,	19,	37,	52,	32,	36,	31,	30.
ind. $\mu - 2$. ind. $(1+\mu) \equiv$ (mod. 5)	2,	0,	4,	4,	3,	3,	0,	4,	3,	4,	4,	1,	0,	0,	3,	3,	0,	4,	1 . . .	

Aus der 3ten Horizontalreihe dieser Tabelle findet man durch einfaches Abzählen:

$$A_0 = 12,\ A_1 = 12,\ A_2 = 6,\ A_3 = 15,\ A_4 = 14$$

also:

$$A_0 + A_1 + A_2 + A_3 + A_4 = 59$$

der Gleichung (43) gemäss, und:

$$\psi_1(\alpha) = 12 + 12\alpha + 6\alpha^2 + 15\alpha^3 + 14\alpha^4.$$

10. Die Principien zur directen Auflösung der Kreistheilungs- und Periodengleichungen, welche wir in Nr. 1—4 dieser Vorlesung aus einander gesetzt haben, finden sich schon in Gauss' Disqu. arithm. art. 360. Nach ihm hat Lagrange (in seinem traité de la résolution des équations numériques 2e édition) den Gegenstand wieder aufgenommen und Gauss' Methode zu vereinfachen geglaubt, jedoch bemerkt Dieser in der bereits angeführten Abhandlung im 2. Bd. seiner Werke mit Recht, dass die Vereinfachung nur scheinbar sei und einen Uebelstand mit sich führe, welchen er selbst vermieden hatte. Die Zurückführung der Auflösung auf die Functionen $\psi_n(\omega^h)$ ist Gauss gleichfalls bekannt gewesen, wie aus dieser Abhandlung, welche zwar erst nach seinem Tode publicirt worden, aber bereits im Jahre 1808 geschrieben ist, zu ersehen ist. Es muss jedoch bemerkt werden, dass lange vor der Publication dieser Arbeit Jacobi zu denselben Resultaten gelangt war, und sie sowohl in seinen Vorlesungen als auch in der in Nr. 8 erwähnten Abhandlung bekannt gemacht hatte. Die ersten Publicationen, welche die in dieser Vorlesung dargestellten Betrachtungen zum Gegenstand haben, rühren von Eisenstein und Cauchy her.*)

Wir beschliessen diese Vorlesung mit der Berechnung einiger einfachen Beispiele.

1) Stellen wir uns zuerst die Aufgabe, die Gleichung

---

*) Eisenstein, Beiträge zur Kreistheilung in Crelle's J. Bd. 27 und Cauchy in seinem grossen mémoire sur la théorie des nombres in den Mém. de l'Acad. des Sciences, vol. 17, Jahrg. 1840. Diese sehr inhaltsreiche Abhandlung Cauchy's, deren Resultate grossentheils mit den von Jacobi erhaltenen übereinstimmen, ist vom 31. Mai 1830 datirt und in ihrem Hauptinhalt bereits im Jahre 1831 im Bulletin de Férussac veröffentlicht worden. S. auch Lebesgue in Liouv. J. Bd. 19, démonstration de quelques formules d'un mémoire de M. Jacobi.

$$\frac{x^5-1}{x-1}=0$$

aufzulösen. Dazu wählen wir ω als primitive Wurzel der Gleichung $x^4=1$, also $\omega=i$, und bestimmen den Ausdruck (i, r), welcher nach Formel (33) durch Auflösung der reinen Gleichung 4ten Grades

$$(i, r)^4=-5\,.\,\psi_1(i)\,\psi_2(i)$$

gefunden wird, während

$$\psi_1(i)=\sum_1^3 i^{\text{ind.}\mu-2\,\text{ind.}(1+\mu)},\qquad \psi_2(i)=\sum_1^3 i^{\text{ind.}\mu-3\,\text{ind.}(1+\mu)}$$

ist. Setzt man nun $g=2$, so findet man die Tabelle:

$$\begin{array}{rl} \mu = & 1,\ 2,\ 3,\ 4 \\ \text{ind.}\,\mu = & 0,\ 1,\ 3,\ 2 \\ \text{ind.}\,(1+\mu) = & 1,\ 3,\ 2 \\ \text{ind.}\,\mu-2\,\text{ind.}\,(1+\mu) \equiv & 2,\ 3,\ 3 \\ \text{ind.}\,\mu-3\,\text{ind.}\,(1+\mu) \equiv & 1,\ 0,\ 1 \end{array}\Bigg\}\ (\text{mod. } 4)$$

also

$$\psi_1(i)=-(1+2i),\ \psi_2(i)=1+2i$$
$$(i, r)^4=5\,.\,(1+2i)^2.$$

Ferner geht aus den Gleichungen (30) und (32) leicht

$$(i, r)^2=(-1, r)\,.\,\psi_1(i),\ \text{also}\ (-1, r)=-\sqrt{5}$$
$$(i,r)^3=(-i,r)\,.\,\psi_1(i)\,\psi_2(i),\ \text{also}\ (-i,r)=-(i,r)\,.\,\frac{\sqrt{5}}{1+2i}$$

hervor, und endlich liefert daher die Gleichung (21) für die gesuchte Wurzel den Werth:

$$r=\frac{1}{4}\left(-1-\sqrt{5}+(i,\ r)\,.\left[1-\frac{\sqrt{5}}{1+2i}\right]\right),$$

welcher indessen, da nach leichten Reductionen

$$(i,\ r)^2\,.\left(1-\frac{\sqrt{5}}{1+2i}\right)^2=-(10-2\sqrt{5})$$

gefunden wird, auch in folgender Gestalt geschrieben werden kann:

$$r=\frac{1}{4}\left(-1-\sqrt{5}+i\sqrt{10-2\sqrt{5}}\right),$$

[we]lcher er bis auf das willkürliche Vorzeichen von $\sqrt{5}$ mit [d]er 7. Vorlesung gefundenen übereinstimmt.

[Zw]eitens soll für den Fall $p=11$ die reine Gleichung

5ten Grades, durch welche die zweigliedrigen Perioden bestimmt werden, aufgestellt und die Ausdrücke dieser Perioden angegeben werden. — Indem man unter r eine Wurzel der Gleichung

$$\frac{x^{11}-1}{x-1}=0,$$

unter $\eta_0, \eta_1, \eta_2, \eta_3, \eta_4$ die zweigliedrigen Perioden, unter α endlich eine primitive Wurzel der Gleichung $x^5 = 1$ versteht, wird die 5te Potenz des Ausdruckes

$$(\alpha, \eta_0) = \eta_0 + \alpha\eta_1 + \alpha^2\eta_2 + \alpha^3\eta_3 + \alpha^4\eta_4$$

nach Formel (34) mittels der Gleichung

$$(\alpha, \eta_0)^5 = 11 \,.\, \psi_1(\alpha)\,\psi_2(\alpha)\,\psi_3(\alpha)$$

gegeben, während

$$\psi_1(\alpha) = \sum_1^9 \alpha^{\text{ind.}\mu - 2\,\text{ind.}(1+\mu)}$$

$$\psi_2(\alpha) = \sum_1^9 \alpha^{\text{ind.}\mu - 3\,\text{ind.}(1+\mu)} = \sum_1^9 \alpha^{\text{ind.}\mu + 2\,\text{ind.}(1+\mu)}$$

$$\psi_3(\alpha) = \sum_1^9 \alpha^{\text{ind.}\mu - 4\,\text{ind.}(1+\mu)} = \sum_1^9 \alpha^{\text{ind.}\mu + \text{ind.}(1+\mu)}$$

sind. Für die primitive Wurzel $g = 2$ findet man folgende Tabelle:

$$\begin{aligned}
\mu &= 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10\\
\text{ind.}\,\mu &= 0,\ 1,\ 8,\ 2,\ 4,\ 9,\ 7,\ 3,\ 6,\ 5\\
\text{ind.}\,(1+\mu) &= 1,\ 8,\ 2,\ 4,\ 9,\ 7,\ 3,\ 6,\ 5\\
\text{ind.}\,\mu + \text{ind.}\,(1+\mu) &\equiv 1,\ 4,\ 0,\ 1,\ 3,\ 1,\ 0,\ 4,\ 1\\
\text{ind.}\,\mu + 2\,\text{ind.}\,(1+\mu) &\equiv 2,\ 2,\ 2,\ 0,\ 2,\ 3,\ 3,\ 0,\ 1\\
\text{ind.}\,\mu - 2\,\text{ind.}\,(1+\mu) &\equiv 3,\ 0,\ 4,\ 4,\ 1,\ 0,\ 1,\ 1,\ 1
\end{aligned}\Bigg\}\ (\text{mod. } 5),$$

nach welcher man die Functionen $\psi_1(\alpha)$, $\psi_2(\alpha)$, $\psi_3(\alpha)$ berechnen kann. Mit Hilfe der Gleichung

$$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$$

erhält man

$$(45)\quad \begin{cases}
\psi_1(\alpha) = 2 + 4\alpha + \alpha^3 + 2\alpha^4 = 2\alpha - 2\alpha^2 - \alpha^3\\
\psi_2(\alpha) = 2 + \alpha + 4\alpha^2 + 2\alpha^3 = -\alpha + 2\alpha^2 - 2\alpha^4\\
\psi_3(\alpha) = 2 + 4\alpha + \alpha^3 + 2\alpha^4 = 2\alpha - 2\alpha^2 - \alpha^3
\end{cases}$$

also auch

$$(46)\qquad \psi_1(\alpha)\,\psi_2(\alpha) = 10\alpha + 6\alpha^2 + 12\alpha^3 + 3\alpha^4$$

$$(47)\qquad \psi_1(\alpha)\,\psi_2(\alpha)\,\psi_3(\alpha) = 6\alpha + 41\alpha^2 + 16\alpha^3 + 26\alpha^4.$$

Nach dem letzten Werthe wird die gesuchte Gleichung die

folgende sein:

$$(48) \qquad (\alpha, \eta_0)^5 = 66\alpha + 451\alpha^2 + 176\alpha^3 + 286\alpha^4.$$

Nach Auflösung derselben, welche zu bewerkstelligen bleibt, ist (α, η_0) als bekannt anzusehen, und dann liefert die Formel (35) diese Gleichungen:

$$(\alpha^2, \eta_0) = \frac{W^2}{\psi_1(\alpha)}, \quad (\alpha^3, \eta_0) = \frac{W^3}{\psi_1(\alpha)\psi_2(\alpha)}, \quad (\alpha^4, \eta_0) = \frac{W^4}{\psi_1(\alpha)\psi_2(\alpha)\psi_3(\alpha)},$$

in denen W zur Abkürzung für (α, η_0) geschrieben ist.

Nun haben wir vorher für die primitiven Wurzeln der Gleichung $x^5 = 1$ den allgemeinen Ausdruck gefunden

$$\alpha = \frac{1}{4}\left(-1 - \sqrt{5} + i\,.\sqrt{10 - 2\sqrt{5}}\right),$$

aus welchem ohne Schwierigkeit durch Potenzirung die Gleichungen folgen:

$$\alpha^2 = \frac{1}{4}\left(-1 + \sqrt{5} - i\,.\sqrt{10 + 2\sqrt{5}}\right)$$

$$\alpha^3 = \frac{1}{4}\left(-1 + \sqrt{5} + i\,.\sqrt{10 + 2\sqrt{5}}\right)$$

$$\alpha^4 = \frac{1}{4}\left(-1 - \sqrt{5} - i\,.\sqrt{10 - 2\sqrt{5}}\right).$$

Durch Substitution dieser Werthe in die Gleichungen (45) bis (48) erhält man die folgenden:

$$\psi_1(\alpha) = \frac{1}{4}\left(1 - 5\sqrt{5} + 2i\sqrt{10 - 2\sqrt{5}} + i\sqrt{10 + 2\sqrt{5}}\right)$$

$$\psi_1(\alpha)\psi_2(\alpha) = \frac{1}{4}\left(-31 + 5\sqrt{5} + 7i\sqrt{10 - 2\sqrt{5}} + 6i\sqrt{10 + 2\sqrt{5}}\right)$$

$$\psi_1(\alpha)\psi_2(\alpha)\psi_3(\alpha) = \frac{1}{4}\left(-89 - 25\sqrt{5} - 20i\sqrt{10 - 2\sqrt{5}} - 25i\sqrt{10 + 2\sqrt{5}}\right)$$

$$W = \sqrt[5]{\frac{11}{4}\left(-89 - 25\sqrt{5} - 20i\sqrt{10 - 2\sqrt{5}} - 25i\sqrt{10 + 2\sqrt{5}}\right)},$$

welche endlich in die Formel

$$\eta_0 = \frac{1}{5}\left(-1 + W + \frac{W^2}{\psi_1(\alpha)} + \frac{W^3}{\psi_1(\alpha)\psi_2(\alpha)} + \frac{W^4}{\psi_1(\alpha)\psi_2(\alpha)\psi_3(\alpha)}\right)$$

einzusetzen wären, um den allgemeinen Ausdruck der zweigliedrigen Perioden zu finden.*)

*) Vgl. hiezu Gauss, circa aequat. puras ulterior evolutio, art. 13; Lagrange, résolution des équations numériques, 3. édition, Note 14 No. 24—36.

Neunte Vorlesung.

Anwendung der Kreistheilung auf die Theorie der quadratischen Reste.

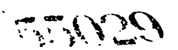
Bis hierher haben wir ausschliesslich das Ziel verfolgt, die Aufgabe der Kreistheilung selbst und die äquivalente algebraische Aufgabe, nämlich die algebraische Auflösung der Kreistheilungsgleichung, zu absolviren. Nur wo die Methode, welche zur Auflösung dieser letztern gegeben wurde, auf gewissen Eigenschaften der ganzen Zahlen wesentlich beruht, sind wir dazu geführt worden, die höhere Arithmetik in den Kreis der Betrachtung zu ziehen und als Hilfsmittel zu gebrauchen. Wenn aber die Kreistheilung auf der einen Seite die Hilfe der Zahlentheorie in Anspruch nimmt, so erweist sie sich auf der andern Seite, wie nun in den folgenden Vorlesungen gezeigt werden soll, als eine sehr ergiebige Quelle, aus der eine grosse Reihe der schönsten Sätze jener Wissenschaft abgeleitet werden kann. Und eine so wunderbare Wechselbeziehung findet zwischen diesen beiden Gebieten statt, dass dann wieder die rein arithmetischen Untersuchungen über die Natur der complexen Zahlen, welche aus Einheitswurzeln gebildet sind, zur Erkenntniss von der wahren Zusammensetzung dieser letztern, also erst zur vollkommenen Lösung des uns gestellten Problems der Kreistheilung hinführen werden.

Von den Anwendungen, welche von der Kreistheilung bisher auf die höhere Arithmetik gemacht worden sind, betreffen die wichtigsten die Theorie der Potenzreste, mit welcher die Zerlegung der Zahlen in die Summe von Quadratzahlen in nahem Zusammenhange steht. Wir beginnen diese Untersuchungen mit der Lehre von den quadratischen Resten, schicken jedoch einige allgemeine Betrachtungen vorauf.

1. Wenn m eine relative Primzahl zu p ist, für welche die Congruenz

$$x^n \equiv m \pmod{p} \tag{1}$$

eine Auflösung gestattet, so heisse m ein n^{ter} Potenzrest (mod. p), im andern Falle werden wir sagen, m sei Nichtrest von p. Wir werden uns auf ungerade Primzahlmoduln p



und auf solche Fälle beschränken, in denen n ein Theiler von $p-1$ ist, auf welche die übrigen leicht zurückführbar sind.

Bezeichnet μ den index von m, so dass $m \equiv g^{\mu}$ (mod. p) ist, so ergiebt sich, wenn die Congruenz (1) möglich ist, durch ihre Erhebung zur $\frac{p-1}{n}^{ten}$ Potenz:

$$1 \equiv g^{\mu . \frac{p-1}{n}} \pmod{p},$$

weil, wenn m nicht durch p theilbar ist, es auch x nicht sein kann; diese Congruenz lehrt aber, dass $\mu =$ ind. m durch n theilbar sein muss, da g zum Exponenten $p-1$ (mod. p) gehört. Umgekehrt, wenn dies der Fall und $\mu = n\nu$ ist, so findet man:

$$m \equiv (g^{\nu})^n \pmod{p}$$

d. h. m ist ein n^{ter} Potenzrest von p. Hiernach sind unter allen incongruenten Zahlen

$$1, g, g^2, g^3, \ldots . g^{p-2}$$

die folgenden:

$$g^n, g^{2n}, g^{3n}, \ldots . g^{\frac{p-1}{n}.n}$$

n^{te} Potenzreste (mod. p), alle übrigen Nichtreste. Die Anzahl der incongruenten n^{ten} Potenzreste beträgt daher $\frac{p-1}{n}$. Die nothwendige und ausreichende Bedingung dafür, dass m ein n^{ter} Potenzrest sei, lässt sich offenbar auch durch die Congruenz

$$(2) \qquad m^{\frac{p-1}{n}} \equiv 1 \pmod{p}$$

aussprechen, welche nicht nur befriedigt ist, sobald der ind. m durch n theilbar ist, sondern auch umgekehrt diese Theilbarkeit erheischt.

2. Wird speciell n gleich Zwei gesetzt, eine Zahl, welche stets Theiler von $p-1$ ist, so heisst eine durch p nicht theilbare Zahl m quadratischer Rest oder Nichtrest (mod. p), je nachdem die Congruenz

$$x^2 \equiv m \pmod{p}$$

möglich oder unmöglich ist, d. h. (nach Formel (2)), je nachdem die Congruenz

$$m^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

stattfindet oder nicht. Da nun für jede solche Zahl m der Fermat'sche Satz:

$$m^{p-1} - 1 \equiv 0 \pmod{p}$$

erfüllt, also einer der Factoren $m^{\frac{p-1}{2}} - 1$, $m^{\frac{p-1}{2}} + 1$, in welche $m^{p-1} - 1$ zerfällt, durch p theilbar sein muss, so wird jeder quadratische Nichtrest der Congruenz

$$m^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

genügen müssen, wodurch wir zum folgenden (sogenannten Euler'schen) Criterium gelangen:

Eine Zahl m ist quadratischer Rest oder Nichtrest von p, je nachdem in der Congruenz:

$$m^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p} \tag{3}$$

das obere oder untere Zeichen zu wählen ist.

Die Anzahl der (incongruenten) quadratischen Reste ist der der Nichtreste gleich, jene können durch die Potenzen $1, g^2, g^4, \ldots\ldots g^{p-3}$, diese durch die Potenzen $g, g^3, g^5 \ldots\ldots g^{p-2}$ dargestellt werden.

Führen wir mit Legendre zur Bezeichnung des quadratischen Characters einer Zahl m (mod. p), dem gemäss sie quadratischer Rest oder Nichtrest von p ist, das Symbol

$$\left(\frac{m}{p}\right)$$

ein, das wir je nach diesen Fällen der positiven oder negativen Einheit gleichsetzen, so ist stets

$$m^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right) \pmod{p}. \tag{4}$$

Congruente Zahlen haben offenbar gleichen quadratischen Character, in Zeichen: es ist

$$\left(\frac{m'}{p}\right) = \left(\frac{m}{p}\right), \text{ wenn } m' \equiv m \pmod{p}. \tag{5}$$

Sind ferner m, m' zwei gleiche oder verschiedene, durch p nicht theilbare Zahlen, so folgt aus den Congruenzen:

$$m^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right), \quad m'^{\frac{p-1}{2}} \equiv \left(\frac{m'}{p}\right) \pmod{p}$$

die dritte:

$$(mm')^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right) \cdot \left(\frac{m'}{p}\right) \pmod{p}$$

und folglich auch:

$$\left(\frac{mm'}{p}\right) \equiv \left(\frac{m}{p}\right) \cdot \left(\frac{m'}{p}\right),$$

was, wie mit Leichtigkeit daraus folgt, dass beide Seiten einen der Werthe $+1$ oder -1 haben, und p von 2 verschieden vorausgesetzt ist, die Gleichung:

$$(6) \qquad \left(\frac{mm'}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{m'}{p}\right)$$

nach sich zieht, welche lehrt, dass das Product aus zwei quadratischen Resten oder aus zwei quadratischen Nichtresten stets ein quadratischer Rest, dagegen das Product aus einem Reste in einen Nichtrest immer ein quadratischer Nichtrest ist. Da wegen derselben Gleichung der quadratische Character eines Productes nur durch die Charactere der Factoren bestimmt wird, so können wir uns in der Folge auf die einfachsten Factoren, d. i. weil m sowohl positiv als negativ, gerade als ungerade vorausgesetzt werden darf, auf die drei Fälle:

$$m = -1, \quad m = 2, \quad m = q$$

beschränken, wo q eine von p verschiedene ungerade Primzahl bedeutet. Es handelt sich also um die Bestimmung der Werthe für die drei Symbole:

$$\left(\frac{-1}{p}\right), \left(\frac{2}{p}\right), \left(\frac{q}{p}\right).$$

Der erste dieser drei Werthe ergiebt sich unmittelbar aus der Definition des Legendre'schen Zeichens oder aus der Congruenz (4), nach welcher

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

oder vielmehr

$$(7) \qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

gefunden wird.

Hiernach ist -1 von jeder Primzahl von der Form

$4n+1$ quadratischer Rest, von jeder Primzahl von der Form $4n+3$ quadratischer Nichtrest.

Zur Bestimmung des dritten Symboles dient ein berühmter Satz, der seiner eigenthümlichen Natur nach von Legendre als Reciprocitätsgesetz bezeichnet worden ist, während Gauss ihn in Hinsicht seiner grossen Wichtigkeit das theorema fundamentale der Theorie der quadratischen Reste nennt. Er kann durch folgende Gleichung ausgedrückt werden:

$$(8) \qquad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

sagt also aus: dass die beiden Symbole $\left(\frac{p}{q}\right)$, $\left(\frac{q}{p}\right)$ gleichen Werth haben, wenn unter den beiden Primzahlen p, q wenigstens eine von der Form $4k+1$ ist (wodurch dann der Exponent von -1 in jener Formel gerade, die Potenz gleich $+1$ wird), dagegen entgegengesetzten Werth, wenn beide Primzahlen die Form $4k+3$ haben (denn in diesem Fall ist der Exponent $\frac{p-1}{2} \cdot \frac{q-1}{2}$ ungerade).

Der auf das Symbol $\left(\frac{2}{p}\right)$ bezügliche Satz soll als Ergänzungssatz zum Reciprocitätsgesetze später durch Betrachtungen bewiesen werden, welche zwar dem Wesen nach den beim Beweise des Reciprocitätsgesetzes zu benützenden ähnlich sind, aber passend mit einer andern Reihe von Untersuchungen in Verbindung gesetzt werden.

3. Das Reciprocitätsgesetz ist zum ersten Male in voller Strenge von Gauss in den Disqu. arithm. art. 135 sqq. bewiesen worden*). Diesem ersten Beweise, zu welchem Gauss erst nach angestrengtestem Nachdenken gelangt ist, wie er selbst erwähnt, hat er später noch fünf andere Beweise folgen lassen, von denen uns der 4te**) und 6te***) besonders interessiren, weil die Quelle derselben eine Formel aus der Kreistheilung ist. Auch alle später noch gegebenen Beweise gründen sich auf diese Formel, selbst wo es nicht der Fall, vielmehr der Beweis ganz arith-

*) Vgl. art. 151 ebd.

**) Gauss, summatio quarundam serierum singularium in s. Op. Bd. II, pag. 11.

***) Ebendas. p. 55.

metischer Natur zu sein scheint, wie derjenige, welchen Eisenstein in Crelle's Journal Bd. 27, pag. 322 mitgetheilt hat.*) Lebesgue hat in einer interessanten Arbeit**) diese verschiedenen Beweise in ihrem gegenseitigen Verhältniss geprüft, und wir wollen sie sogleich unter demselben Gesichtspunkte, wenn auch in mancher Beziehung von Lebesgue abweichend, betrachten.

Zunächst aber handelt es sich darum, die Grundformel aus der Kreistheilung abzuleiten. — Gehen wir aus von der Formel:

$$(\omega^h, r) = \sum_{\mu=1}^{\mu=p-1} \omega^{h\,\mathrm{ind.}\mu} \,.\, r^\mu$$

und setzen $h = \frac{p-1}{2}$, so wird $\omega^{\frac{p-1}{2}} = -1$, $\omega^{\frac{p-1}{2}.\mathrm{ind.}\mu} = (-1)^{\mathrm{ind.}\mu}$ d. h. 1 oder — 1 sein, jenachdem ind. μ gerade oder ungerade, also nach Nr. 2, jenachdem μ quadratischer Rest oder Nichtrest von p ist. Bezeichnet man daher mit α, β resp. die quadratischen Reste und Nichtreste aus der Reihe 1, 2, 3, . . . $(p-1)$ und setzt

$$\left(\omega^{\frac{p-1}{2}}, r\right) = (-1, r) = S, \tag{9}$$

so findet man:

$$S = \sum_\alpha r^\alpha - \sum_\beta r^\beta \tag{10}$$

oder, da $\left(\frac{s}{p}\right) = \pm 1$ ist, jenachdem s quadratischer Rest oder Nichtrest von p ist,

$$S = \sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right) . r^s. \tag{11}$$

Zunächst sei noch eine andere Form dieses Ausdruckes erwähnt. Offenbar besteht die Gleichung:

$$0 = 1 + \sum_\alpha r^\alpha + \sum_\beta r^\beta, \tag{12}$$

---

*) Neuer und elementarer Beweis des Legendre'schen Reciprocitätsgesetzes.

**) Démonstration nouvelle et élémentaire de la loi de réciprocité de Legendre, par M. Eisenstein, précédée et suivie de remarques sur d'autres démonstrations, qui peuvent être tirées du même principe, in Liouville's Journal Bd. 12.

da die Zahlen α, β zusammengenommen die Reihe 1, 2, 3, ... $p-1$ erschöpfen. Durch Addition dieser Gleichung zur Gleichung (10) und vermittelst der Bemerkung, dass zwei Zahlen s und $p-s$ congruente Quadrate haben, da

$$(p-s)^2 = p^2 - 2ps + s^2 \equiv s^2 \pmod{p}$$

ist, dass also die kleinsten Reste der Quadratzahlen

$$1^2, 2^2, 3^2, \ldots (p-1)^2$$

(mod. p) die quadratischen Reste α und jeden genau zweimal liefern werden, ergiebt sich zuerst:

$$S = 1 + 2 \cdot \sum_{\alpha} r^{\alpha} \tag{13}$$

sodann:

$$S = \sum_{s=0}^{s=p-1} r^{s^2}. \tag{14}$$

Führen wir noch die Bezeichnungen ein:

$$\sum_{\alpha} r^{\alpha} = U, \quad \sum_{\beta} r^{\beta} = V,$$

so nehmen die Gleichungen (10) und (12) die Gestalt an:

$$U - V = S \tag{10a}$$

$$1 + U + V = 0 \tag{12b}$$

und ergeben:

$$U = \frac{-1 + S}{2}, \quad V = \frac{-1 - S}{2}. \tag{15}$$

Das Quadrat des Ausdrucks S ist sehr leicht zu ermitteln. Denn da $\omega^{-\frac{p-1}{2}} = \omega^{\frac{p-1}{2}}$, also

$$\left(\omega^{\frac{p-1}{2}}, r\right) = \left(\omega^{-\frac{p-1}{2}}, r\right)$$

ist, so liefert die Formel (29) der vorigen Vorlesung, indem man $h = \frac{p-1}{2}$ setzt, sofort die Gleichung:

$$S^2 = (-1)^{\frac{p-1}{2}} \cdot p. \tag{16}$$

Hieraus folgt der Werth von S bis auf das Vorzeichen, nämlich

$$S = \pm \sqrt{(-1)^{\frac{p-1}{2}} \cdot p}, \tag{17}$$

aber zu entscheiden, welches Vorzeichen in dieser Formel zu wählen sei, ist nicht einfach, sondern erst den Bemühungen der grössten Mathematiker gelungen. Zunächst ist klar, dass das Vorzeichen wesentlich davon abhängt, welche Wurzel der Kreistheilungsgleichung unter r verstanden wird. Denn, ersetzt man r durch r^k, so geht S über in:

$$\sum_{\alpha} r^{\alpha k} - \sum_{\beta} r^{\beta k}.$$

Wenn nun k quadratischer Rest von p ist, so bilden die $\frac{p-1}{2}$ Zahlen αk ebensoviel incongruente quadratische Reste, stimmen also, von Vielfachen von p abgesehen, mit den Zahlen α überein, desgleichen die Zahlen βk mit den Nichtresten β, der neue Ausdruck ist daher gleich S. Wenn dagegen k ein quadratischer Nichtrest von p ist, so werden die Zahlen αk mit den Nichtresten β, die Zahlen βk mit den Resten α, von Vielfachen von p abgesehen, übereinstimmen, die beiden Theile der Summe S also sich vertauschen und S in $-S$ übergehen. Definirt man daher S_k durch die Gleichung:

$$S_k = \sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right) \cdot r^{ks}, \tag{18}$$

so wird stets:

$$S_k = \left(\frac{k}{p}\right) \cdot S \tag{19}$$

sein, wenn k nicht durch p theilbar ist.

Um demnach über das Vorzeichen in der Formel (17) zu entscheiden, muss vor Allem unter r eine bestimmte Wurzel verstanden werden, und es soll hinfort stets, wo nicht das Gegentheil bemerkt wird,

$$r = \cos\frac{2\pi}{p} + i \sin\frac{2\pi}{p}$$

angenommen werden. Gauss hat seine oben citirte Abhandlung summatio etc. hauptsächlich zur Lösung der vorliegenden Frage geschrieben, während der Beweis des Reciprocitätsgesetzes, der sich in derselben befindet, mehr beiläufig erhalten wird. Dirichlet*) hat dieselbe Untersuchung mittelst sehr feiner Betrachtungen aus

*) Dirichlet, sur l'usage des intégrales définies dans la sommation des séries finies ou infinies, Cr. J. Bd. 17.

der Lehre von den bestimmten Integralen geführt. Am Einfachsten gelangt man zum gewünschten Ziele durch Betrachtungen, welche Kronecker angegeben hat*), und denen wir hier folgen wollen.

4. Da nach Nr. 7 der 3. Vorlesung die Potenzen r^2, r^4, r^6, ... $r^{2(p-1)}$ alle Wurzeln der Kreistheilungsgleichung bilden, so ist

$$(x-r^2)(x-r^4)\ldots(x-r^{2(p-1)}) = x^{p-1}+x^{p-2}+\ldots+x+1$$

also für $x=1$:

$$(1-r^2)(1-r^4)\ldots(1-r^{2(p-1)}) = p,$$

woraus sich durch Multiplication mit

$$r^{-1}.r^{-2}.r^{-3}\ldots r^{-(p-1)} = r^{-p.\frac{p-1}{2}} = 1$$

die Gleichung:

$$(r^{-1}-r)(r^{-2}-r^2)\ldots(r^{-p+1}-r^{p-1}) = p$$

ergiebt. Da aber:

$$(20)\quad r^{-p+2}-r^{p-2} = r^2-r^{-2},\ r^{-p+4}-r^{p-4} = r^4-r^{-4},\ \ldots\ r^{-1}-r = r^{p-1}-r^{-p+1}$$

ist, kann man jene Gleichung auch in folgender Gestalt schreiben:

$$[(r-r^{-1})(r^3-r^{-3})\ldots(r^{p-2}-r^{-p+2})]^2 = (-1)^{\frac{p-1}{2}}.p.$$

Ist nun erstens $p=4n+1$, so ergiebt sich

$$\prod_{h=1}^{h=\frac{p-1}{2}}(r^{2h-1}-r^{-2h+1}) = \pm\sqrt{p}.$$

Nach der über r getroffenen Bestimmung ist

$$r^{2h-1}-r^{-2h+1} = 2i.\sin\frac{2(2h-1)\pi}{p}$$

also

$$(21)\quad \prod_{h=1}^{h=\frac{p-1}{2}}(r^{2h-1}-r^{-2h+1}) = (2i)^{\frac{p-1}{2}}.\sin\frac{2\pi}{p}.\sin 3.\frac{2\pi}{p}\ldots\sin(p-2).\frac{2\pi}{p}$$

$$= 2^{\frac{p-1}{2}}.i^{\frac{p-1}{2}}.(-1)^{\frac{p-1}{4}}.\sin\frac{2\pi}{p}.\sin\frac{4\pi}{p}\ldots\sin\frac{(p-1)\pi}{p},$$

---

*) Kronecker, sur une formule de Gauss in Liouv. J., Bd. 1, 2. série.

wo rechts alle sinus positiv sind, da die Argumente derselben kleiner als π bleiben; da nun $i^{\frac{p-1}{2}} . (-1)^{\frac{p-1}{4}} = (-1)^{\frac{p-1}{2}} = 1$ ist, so hat das Product einen positiven Werth, also ergiebt sich:

$$\prod_{h=1}^{h=\frac{p-1}{2}} (r^{2h-1} - r^{-2h+1}) = +\sqrt{p}.$$

Ist zweitens $p = 4n + 3$, so findet man zunächst:

$$\prod_{h=1}^{h=\frac{p-1}{2}} (r^{2h-1} - r^{-2h+1}) = \pm i\sqrt{p}.$$

Durch dieselbe Transformation der Formel (21) jedoch ergiebt sich dies Product gleich

$$2^{\frac{p-1}{2}} \cdot i^{\frac{p-1}{2}} . (-1)^{\frac{p-3}{4}} . \sin\frac{2\pi}{p} . \sin\frac{4\pi}{p} \dots \sin\frac{(p-1)\pi}{p}$$

hat also dasselbe Vorzeichen wie $i^{\frac{p-1}{2}+\frac{p-3}{2}} = i^{p-2} = i$, und man erhält:

$$\prod_{h=1}^{h=\frac{p-1}{2}} (r^{2h-1} - r^{-2h+1}) = + i\sqrt{p}.$$

Demnach ist allgemein:

$$(22) \quad (r - r^{-1}) . (r^3 - r^{-3}) \dots (r^{p-2} - r^{-p+2}) = +\sqrt{(-1)^{\frac{p-1}{2}} . p}.$$

5. Nachdem dies bewiesen worden, kommt die vorher gestellte Frage darauf hinaus, ob in der Gleichung:

$$(23) \qquad \sum_\alpha r^\alpha - \sum_\beta r^\beta = \varepsilon . \prod_{h=1}^{h=\frac{p-1}{2}} (r^{2h-1} - r^{p-2h+1})$$

das Zeichen ε, welches entweder $+1$ oder -1 sein muss, diesen oder jenen Werth hat. Diese Relation lehrt aber, dass die algebraische Gleichung

$$\sum_\alpha x^\alpha - \sum_\beta x^\beta - \varepsilon . \prod_{h=1}^{h=\frac{p-1}{2}} (x^{2h-1} - x^{p-2h+1}) = 0$$

mit offenbar ganzzahligen Coëfficienten durch die Wurzel r und

folglich durch alle Wurzeln der irreductibeln Kreistheilungsgleichung befriedigt wird, die ganze Function auf der linken Seite also durch

$$x^{p-1} + x^{p-2} + \dots + x + 1$$

theilbar sein muss, und da der Gleichung auch durch $x = 1$ Genüge geschieht, so kann man setzen:

$$\sum_\alpha x^\alpha - \sum_\beta x^\beta - \varepsilon \cdot \prod_{h=1}^{h=\frac{p-1}{2}} (x^{2h-1} - x^{p-2h+1})$$
$$= (x^p - 1)(A + Bx + \dots + Kx^k),$$

worin $A, B, \dots K$ ganze Zahlen bedeuten. Für die Unbestimmte x setze man nun e^z, also:

$$(24) \qquad \sum_\alpha e^{\alpha z} - \sum_\beta e^{\beta z} - \varepsilon \cdot \prod_{h=1}^{h=\frac{p-1}{2}} (e^{(2h-1)z} - e^{(p-2h+1)z})$$
$$= (e^{pz} - 1)(A + Be^z + \dots + Ke^{kz}),$$

und entwickle die Exponentialfunctionen in ihre Potenzreihen, dann müssen die Coëfficienten gleicher Potenzen auf beiden Seiten übereinstimmen. Da nun

$$e^{mz} = 1 + mz + \frac{m^2 z^2}{1.2} + \dots$$
$$e^{nz} = 1 + nz + \frac{n^2 z^2}{1.2} + \dots$$

ist, wird die Differenz $e^{mz} - e^{nz}$ die Gestalt haben:

$$(m - n) z (1 + az + \dots),$$

weil in der Differenz der allgemeinen Glieder beider Reihen:

$$\frac{m^k z^k}{1.2 \dots k} - \frac{n^k z^k}{1.2 \dots k} = \frac{z^k}{1.2 \dots k}(m^k - n^k),$$

der Factor

$$m^k - n^k = (m - n)(m^{k-1} + m^{k-2} n + \dots + mn^{k-2} + n^{k-1})$$

also durch $m - n$ theilbar ist. Hiernach enthält die Differenz $e^{(2h-1)z} - e^{(p-2h+1)z}$ den Factor $(4h - 2 - p) z$, folglich wird das Product auf der linken Seite der Gleichung (24) die Form annehmen:

$$z^{\frac{p-1}{2}} \cdot \prod_{h=1}^{h=\frac{p-1}{2}} (4h - 2 - p) \cdot (1 + A'z + \dots).$$

Betrachtet man also den Coëfficienten von $z^{\frac{p-1}{2}}$ auf den beiden Seiten, so ergiebt sich die Gleichheit:

$$\frac{\sum\limits_{\alpha}\alpha^{\frac{p-1}{2}}-\sum\limits_{\beta}\beta^{\frac{p-1}{2}}}{1.2.3\ldots\frac{p-1}{2}}-\varepsilon.\prod_{h=1}^{h=\frac{p-1}{2}}(4h-2-p)=\frac{M}{N},$$

in welcher M, N gewisse ganze Zahlen sind, von denen sich soviel ohne Weiteres aussagen lässt, dass die erstere durch p theilbar ist, weil es die Differenz $e^{pz}-1$ ist, und dass die letztere durch p nicht theilbar ist, da in ihr offenbar nur solche Primfactoren vorkommen können, welche in dem Producte $1.2.3\ldots\ldots\frac{p-1}{2}$, enthalten sind. Man erhält daher aus jener Gleichung die nachstehende Congruenz:

$$\sum_{\alpha}\alpha^{\frac{p-1}{2}}-\sum_{\beta}\beta^{\frac{p-1}{2}}\equiv\varepsilon.1.2.3\ldots\frac{p-1}{2}.\prod_{h=1}^{h=\frac{p-1}{2}}(4h-2-p)\pmod{p}.$$

Nun ist nach dem Euler'schen Criterium $\alpha^{\frac{p-1}{2}}\equiv+1$, $\beta^{\frac{p-1}{2}}\equiv-1 \pmod{p}$, und die Anzahl sowohl der Zahlen α als der Zahlen β beträgt $\frac{p-1}{2}$, ferner ist:

$$\prod_{h=1}^{h=\frac{p-1}{2}}(4h-2-p)=(2-p)(6-p)\ldots.(2p-4-p)$$

$$\equiv 2.6.10\ldots.2(p-2)\equiv 2^{\frac{p-1}{2}}.1.3.5\ldots.(p-2)\pmod{p},$$

also ergiebt sich aus der letzterhaltenen Congruenz

$$p-1\equiv 1\,.\,2\,.\,3\,\ldots.\,(p-1)\,\varepsilon$$

oder nach Wilson's Satz:

$$\varepsilon\equiv 1\pmod{p},$$

woraus $\varepsilon=1$ zu schliessen ist.

Hiernach ist das ungewisse Vorzeichen in der Formel (17) bestimmt, und man hat zu setzen:

$$S=+\sqrt{(-1)^{\frac{p-1}{2}}.p}, \tag{25}$$

woraus nach den Gleichungen (15) noch die Formeln:

$$(26)\quad U = \frac{-1 + \sqrt{(-1)^{\frac{p-1}{2}} \cdot p}}{2}, \qquad V = \frac{-1 - \sqrt{(-1)^{\frac{p-1}{2}} \cdot p}}{2}$$

hervorgehen.

Der Grundgedanke des eben mitgetheilten Beweises kann dahin ausgesprochen werden, dass man zur Entscheidung, welchen der Werthe $+1$ oder -1 die Zahl ε in der Gleichung (23) erhalten müsse, untersucht, welcher dieser Zahlen sie (mod. p) congruent zu setzen ist. Auf demselben Grundgedanken beruht ein anderer, von Cauchy herrührender Beweis*), jedoch ist das Mittel, welches Derselbe anwendet, um den Rest von ε (mod. p) zu bestimmen, ein ganz anderes, und obgleich sehr interessant, doch weniger schnell zum Ziele führend als das von Kronecker angewendete, und besteht darin, dass in der Gleichung (23), nachdem das Product nach Potenzen von r entwickelt und diese unter den $(p-1)^{ten}$ Grad erniedrigt sind, $\left(\frac{h}{p}\right)$ statt r^h substituirt wird. Auch Lebesgue**) hat einen Beweis der Formel (25) gegeben, welcher sich mehr an Gauss' Abhandlung summatio etc. anschliesst. In der letztgenannten Arbeit von Lebesgue finden sich zugleich über den Zusammenhang zwischen den Gauss'schen Reihen und den in der Theorie der elliptischen Functionen von Jacobi betrachteten bemerkenswerthe Aufschlüsse.

6. **Die Formel (25) bildet nun die Grundlage für den Beweis des Reciprocitätsgesetzes.** Dazu ist indessen keineswegs unumgänglich nothwendig, das fragliche Vorzeichen in der Formel (17) zuvor zu bestimmen, vielmehr genügt es, den Absolutwerth von S zu kennen, wie es Gauss in seinem 6ten Beweise gezeigt hat. Zwar legt er diesem nicht sowohl die Summe S zu Grunde, als vielmehr den Ausdruck:

$$\sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right) \cdot x^s,$$

---

*) Liouv. J. Bd. V: méthode simple et nouvelle pour la détermination complète des sommes alternées, formées avec les racines primitives des équations binômes; vgl. in seinem mém. sur la théorie des nombres die Notes 7 bis 11.

**) In dems. Bd. des Liouv. Journals: sommation de quelques séries.

worin x beliebig ist; man erreicht aber eine grosse Vereinfachung, wenn man $x = r$ voraussetzt, und der Beweis kann dann nach Jacobi, Eisenstein und Cauchy folgendermaassen geführt werden*):

Aus der Gleichung (16) folgt durch Erhebung in die $\frac{q-1}{2}$ten Potenz und Multiplication mit S:

$$S^q = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} . p^{\frac{q-1}{2}} . S,$$

worin q eine von p verschiedene ungerade Primzahl bedeute. Setzt man andererseits $k = q$ in der Gleichung (19), so findet man durch Verbindung mit der vorigen Gleichung die folgende:

$$(27) \qquad S^q - S_q = \left[(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} . p^{\frac{q-1}{2}} - \left(\frac{q}{p}\right)\right] . S.$$

Nach dem binomischen Lehrsatze ist aber in dem entwickelten Ausdrucke von

$$S^q - S_q = \left(\sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right) r^s\right)^q - \sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right) . r^{qs},$$

da $\left(\frac{s}{p}\right)^q = \left(\frac{s}{q}\right)$ ist, die q^{ten} Potenzen der einzelnen Glieder der ersten Summe sich also gegen die entsprechenden Glieder der zweiten Summe aufheben, der Coëfficient jeder Potenz von r durch q theilbar. Reducirt man daher in (27) die Exponenten von r auf die Reste $0, 1, 2, \ldots p-2$, so müssen, da nun die Coëfficienten jeder Potenz von r auf beiden Seiten der Gleichung (27) wegen der Irreductibilität der Kreistheilungsgleichung einander gleich zu setzen sind, diejenigen der rechten Seite ebenfalls durch q theilbar, also

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} . p^{\frac{q-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{q}$$

sein. Nun ist $p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) \pmod{q}$, und da nach Substitution dieses Werthes beide Seiten der Congruenz den Werth $+1$ oder -1 erhalten, ergiebt sich die Gleichung

*) S. Jacobi's bereits angeführte Note in Crelle's J. Bd. 30, pag. 172, vgl. Bd. 35, pag. 273; Eisenstein, la loi de réciprocité, tirée des formules de Gauss, sans avoir déterminé préalablement le signe du radical, in Cr. J. Bd. 28, pag. 41; Cauchy in mém. sur la th. des nombres, note 4.

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right),$$

welche das Reciprocitätsgesetz ausspricht.

7. Der bereits citirte Beweis von Eisenstein (Cr. J. Bd. 27, pag. 322) ist zwar von ihm rein arithmetisch dargestellt worden; wenn man aber auf den Ursprung der Zahlen, auf deren Eigenschaften er ihn gründet, zurückgeht, wird man wieder auf den Ausdruck S hingeführt. Diese Zahlen sind nämlich nichts anderes, als die Coëfficienten in der Entwicklung von S^k. Das allgemeine Glied der Entwicklung ist:

$$\left(\frac{s_1}{p}\right)\cdot\left(\frac{s_2}{p}\right)\cdots\cdots\left(\frac{s_k}{p}\right)\cdot r^{s_1+s_2+\cdots\cdots+s_k}$$

wenn unter $s_1, s_2, \ldots\ldots s_k$ gleiche oder ungleiche Zahlen der Reihe $1, 2, 3, \ldots\ldots p-1$ verstanden werden. Setzt man daher, indem man die Summation auf alle diejenigen, gleichen oder ungleichen, Zahlen jener Reihe bezieht, welche der Congruenz:

$$(28)\qquad s_1+s_2+\cdots\cdots+s_k\equiv\alpha\quad\text{mod. } p)$$

Genüge leisten,

$$\sum\left(\frac{s_1}{p}\right)\cdot\left(\frac{s_2}{p}\right)\cdots\cdots\left(\frac{s_k}{p}\right)=A_{k,\alpha},$$

so wird:

$$S^k=A_{k,0}+A_{k,1}\cdot r+A_{k,2}\cdot r^2+\cdots\cdots+A_{k,p-1}\,r^{p-1},$$

und da S für $r=1$ in $\sum_{s=1}^{s=p-1}\left(\frac{s}{p}\right)$ übergeht, also verschwindet, weil die Anzahl der quadratischen Reste, für welche $\left(\frac{s}{p}\right)=+1$ ist, der Anzahl der quadratischen Nichtreste, welche $\left(\frac{s}{p}\right)=-1$ geben, gleich ist, so findet man:

$$(29)\qquad 0=A_{k,0}+A_{k,1}+A_{k,2}+\cdots\cdots+A_{k,p-1}.$$

Für jeden, durch p nicht theilbaren Werth des α kann man aber setzen:

$$\left.\begin{array}{l} s_1\equiv\alpha t_1,\ s_2\equiv\alpha t_2,\ \ldots\ldots s_k\equiv\alpha t_k \\ \text{so dass dann:}\quad t_1+t_2+\cdots\cdots t_k\equiv 1\end{array}\right\}\ (\text{mod. } p)$$

ist; jeder Lösung der Congruenz (28) entspricht also eine Lösung der letzteren und umgekehrt. Da für zwei correspondirende

Lösungen nach (6) die Gleichung

$$\left(\frac{s_1}{p}\right)\cdot\left(\frac{s_2}{p}\right)\ldots\left(\frac{s_k}{p}\right)=\left(\frac{\alpha}{p}\right)^k\cdot\left(\frac{t_1}{p}\right)\cdot\left(\frac{t_2}{p}\right)\ldots\left(\frac{t_k}{p}\right)$$

stattfindet, so wird offenbar

$$(30)\qquad A_{k,\alpha}=\left(\frac{\alpha}{p}\right)^k\cdot A_{k,1}$$

sein.

Aus (29) und (30) folgt nun für ein ungerades k:

$$(30\text{a})\qquad A_{k,0}=0,$$

dagegen geben sie für $k=2$

$$A_{2,\alpha}=A_{2,1},\quad A_{2,0}=-(p-1)A_{2,1},$$

folglich wird

$$S^2=A_{2,0}+A_{2,1}(r+r^2+\ldots+r^{p-1})=A_{2,0}-A_{2,1}=-p\,.\,A_{2,1}$$

d. h.

$$S^2=-p\cdot\sum\left(\frac{s_1}{p}\right)\cdot\left(\frac{s_2}{p}\right),$$

während die Summe auf alle Werthsysteme s_1, s_2 bezogen wird, für welche $s_1+s_2\equiv 1 \pmod{p}$ ist. Das allgemeine Glied dieser Summe bleibt ungeändert, wenn wir es mit $\left(\frac{\sigma_1}{p}\right)^2$ multipliciren; dabei wollen wir aber σ_1 jedesmal so wählen, dass $s_1\sigma_1\equiv 1 \pmod{p}$ wird; setzt man sodann $s_2.\sigma_1\equiv\sigma_2 \pmod{p}$, so wird

$$\left(\frac{s_2}{p}\right)\cdot\left(\frac{\sigma_1}{p}\right)=\left(\frac{\sigma_2}{p}\right),\quad\left(\frac{s_1}{p}\right)\cdot\left(\frac{\sigma_1}{p}\right)=\left(\frac{s_1\sigma_1}{p}\right)=\left(\frac{1}{p}\right)=1,$$

und

$$S^2=-p\,.\sum\left(\frac{\sigma_2}{p}\right).$$

Der Umfang der Summation wird durch die Congruenz $1+\sigma_2\equiv\sigma_1 \pmod{p}$ bestimmt, welche sich aus der zwischen s_1, s_2 stattfindenden durch Multiplication mit σ_1 ergiebt. Nun kann σ_1 nicht Eins sein, denn sonst würde $s_1\equiv 1$, $s_2\equiv 0 \pmod{p}$ werden, während auch s_2 nur eine Zahl der Reihe $1, 2, 3 \ldots p-1$ bedeutet; also durchläuft σ_1 die Werthe $2, 3, \ldots p-1$, und σ_2 die Werthe $1, 2, 3, \ldots p-2$. Daraus folgt die Formel:

$$S^2=p\,.\left(\frac{p-1}{p}\right)=p\cdot\left(\frac{-1}{p}\right),$$

da $\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\left(\frac{3}{p}\right)+\ldots+\left(\frac{p-2}{p}\right)+\left(\frac{p-1}{p}\right)=0$

ist. Wegen der Gleichung (7) endlich gelangen wir so direct zu der Formel:

$$S^2 = (-1)^{\frac{p-1}{2}} \cdot p$$

wieder zurück, welche wir vorher aus der Kreistheilung entnommen hatten.

Nun wissen wir bereits, dass $A_{q,1}$ der Coëfficient von r in der Entwicklung von S^q ist; vergleicht man daher in der Gleichung

(31) $$S^q = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot p^{\frac{q-1}{2}} \cdot S,$$

welche identisch sein muss, da sie vom Grade $p-1$, und wegen $A_{q,0}=0$ durch r theilbar ist, die Coëfficienten von r, so findet man:

(32) $$A_{q,1} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot p^{\frac{q-1}{2}}.$$

Man zeigt aber leicht, dass

$$A_{q,1} = \sum \left(\frac{s_1}{p}\right) \cdot \left(\frac{s_2}{p}\right) \cdots \left(\frac{s_q}{p}\right)$$

(33) $$[\text{während } s_1 + s_2 + \cdots + s_q \equiv 1 \pmod{p}]$$

von der Form $\left(\frac{q}{p}\right) + M.q$ ist, wo unter M eine ganze Zahl verstanden wird. In der That, da $qx \equiv 1 \pmod{p}$ nur eine Auflösung gestattet, so kann es nur ein Glied jener Summe geben, in welchem alle s einander gleich sind; da aus $qx \equiv 1 \pmod{p}$ nach (5) und (6) $\left(\frac{q}{p}\right) \cdot \left(\frac{x}{p}\right) = \left(\frac{1}{p}\right) = 1$, also $\left(\frac{q}{p}\right) = \left(\frac{x}{p}\right)$ hervorgeht, wird das zugehörige Glied der Summe den Werth

$$\left(\frac{x}{p}\right)^q = \left(\frac{x}{p}\right) = \left(\frac{q}{p}\right)$$

haben. Aus jeder andern Auflösung der Congruenz (33) aber ergeben sich, worauf wir weitläufiger nicht eingehen wollen, durch cyclische Vertauschung der Zahlen s noch $q-1$ andere, welche sämmtlich von einander verschiedene Systeme repräsentiren, dem Gliede in der Summe aber gleichen Werth ertheilen, woraus offenbar die Richtigkeit des Behaupteten folgt. Dann ergiebt sich aber weiter:

$$\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot p^{\frac{q-1}{2}} \pmod{q}$$

und, wie vorher, der Beweis des Reciprocitätsgesetzes.

Im Grunde ist dieser Beweis genau der vorige. Denn der Coëfficient von r in S_q ist nach der Gleichung (19) gleich $\left(\frac{q}{p}\right)$.

Also ist $A_{q,1} - \left(\frac{q}{p}\right)$ der Coëfficient von r in der Entwicklung von $S^q - S_q$, und der Unterschied beider Beweise besteht einzig darin, dass die Theilbarkeit dieses Coëfficienten durch q in dem ersten mittels des binomischen Satzes, im zweiten mittels einer etwas andern arithmetischen Betrachtung bewiesen wird.

8. Lebesgue's Beweis, der sich in der in Nr. 3 bereits angeführten Arbeit sowie in einer andern Abhandlung im 2. Bd. des Liouv. Journals*) befindet, ist von dem Eisenstein'schen wesentlich nur dadurch verschieden, dass die Summe S unter der andern Form (14) angewendet wird. Entwickelt man dann nämlich wieder die Potenz S^q, so sind die Coëfficienten der Entwicklung diejenigen Zahlen, aus deren Eigenschaften Lebesgue seinen Beweis ableitet. Ohne denselben hier reproduciren zu wollen, werden wir nur jene Zahlen näher bezeichnen und, was nach dem Vorigen leicht ist, ihre Werthe ermitteln. Da nach (14)

$$S = \sum_{s=0}^{s=p-1} r^{s^2}$$

ist, so wird, wenn wir

$$S^q = B_{q,0} + B_{q,1} \cdot r + B_{q,2} \cdot r^2 + \dots + B_{q,\,p-1}\, r^{p-1}$$

setzen, der Coëfficient $B_{q,a}$ offenbar die Anzahl der Lösungen der Congruenz

(34) $$s_1^2 + s_2^2 + \dots + s_q^2 \equiv a \pmod{p}$$

bezeichnen, in welcher $s_1, s_2, \dots s_q$ gleiche oder verschiedene Zahlen der Reihe $0, 1, 2, \dots p-1$ sein können. Es ist nun zuerst leicht einzusehen, dass $B_{q,a}$ denselben Werth hat für alle quadratischen Reste $a = \alpha$, und wieder denselben Werth für alle quadratischen Nichtreste $a = \beta$. Denn, bedeutet a irgend einen quadratischen Rest oder Nichtrest, so können alle quadratischen Reste resp. Nichtreste in der Form ay^2 gedacht werden, welcher sie (mod. p) congruent sind, wenn y eine passend gewählte, nicht durch p theilbare Zahl ist, da man, wenn a' einen andern quadratischen Rest resp. Nichtrest bezeichnet, eine Zahl z durch die Congruenz $az \equiv a'$ (mod. p) bestimmen kann, welche nach dem 3ten Satze in Nr. 2 nothwendig zu den quadratischen Resten gehört, also dem Quadrate einer gewissen Zahl y (mod. p)

*) Recherches sur les nombres.

congruent sein muss. Bestimmt man sodann die Zahlen t_1, t_2, ... t_q den Congruenzen:

$$t_1 \equiv s_1\, y,\ t_2 \equiv s_2\, y, \ldots\ t_q \equiv s_q\, y \pmod{p}$$

gemäss, so liefert jede Auflösung der Congruenz (34) eine bestimmte Auflösung der folgenden:

$$t_1^2 + t_2^2 + \ldots + t^2_q \equiv a\, y^2 \pmod{p}$$

und umgekehrt, so dass beide gleichviel Auflösungen gestatten.

Indem wir daher die beiden Werthe von $B_{q,a}$ für Reste und Nichtreste resp. mit B_q, B'_q bezeichnen, finden wir:

$$S^q = B_{q,0} + B_q \cdot \sum_\alpha r^\alpha + B'_q \sum_\beta r^\beta,$$

oder mit Hilfe der Gleichung

$$1 + \sum_\alpha r^\alpha + \sum_\beta r^\beta = 0:$$

$$S^q = (B_q - B_{q,0}) \cdot \sum_\alpha r^\alpha + (B'_q - B_{q,0}) \cdot \sum_\beta r^\beta.$$

Da wir nun andererseits aus den Gleichungen (31) und (32)

$$S^q = A_{q,1} \cdot \sum_\alpha r^\alpha - A_{q,1} \cdot \sum_\beta r^\beta$$

schliessen, so liefert die Identität beider Ausdrücke die Gleichungen:

(35) $B_q = B_{q,0} + A_{q,1}$, $B'_q = B_{q,0} - A_{q,1}$, also $B_q + B'_q = 2\, B_{q,0}$.

Da ferner jede Combination der Werthe $s_1, s_2, \ldots s_q$ aus der Reihe $0, 1, 2, \ldots p-1$ für irgend einen Werth von a eine Lösung der Congruenz (34) liefern muss, so muss die Anzahl aller Combinationen gleich der Summe aller Zahlen $B_{q,a}$ sein, und so folgt die Gleichung:

$$B_{q,0} + \frac{p-1}{2}(B_q + B'_q) = p^q,$$

also nach (35) folgende Werthe:

$$(36)\quad \begin{cases} B_{q,0} = p^{q-1} \\ B'_q = p^{q-1} - (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot p^{\frac{q-1}{2}} \\ B_q = p^{q-1} + (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot p^{\frac{q-1}{2}}. \end{cases}$$

9. Einen etwas andern Gang nehmen die beiden Beweise von Liouville und Eisenstein*), welche, was ihr Princip betrifft, unter einander als identisch anzusehen sind. Sie gründen sich auf das Lemma, welches dem 3[ten] und 5[ten] der Gaussischen Beweise zum Grunde liegt. Die absolut kleinsten, zwischen $+\frac{p-1}{2}$ und $-\frac{p-1}{2}$ inclusive liegenden Reste der Reihe

$$1 \cdot q,\ 2 \cdot q,\ 3 \cdot q, \ldots \frac{p-1}{2} \cdot q$$

werden nämlich theils positiv sein — diese nennen wir a_1, a_2, ... a_λ — theils negativ — diese seien $-b_1$, $-b_2$, ... $-b_\mu$, sodass $\lambda + \mu = \frac{p-1}{2}$. Die Zahlen a sowie die Zahlen b sind unter einander verschieden, da jene Multipla von q einander nicht (mod. p) congruent sein können; die $\frac{p-1}{2}$ Zahlen a und b zusammengenommen bilden aber alle Zahlen der Reihe 1, 2, 3, ... $\frac{p-1}{2}$, denn die Zahlen b sind ebenso wie die Zahlen a nicht grösser als $\frac{p-1}{2}$, und kein b kann einem a gleich sein, da sonst ihre Differenz und folglich die Summe derjenigen Multipla von q, denen sie congruent sind, durch p theilbar wäre, was offenbar für keine zwei jener Multipla möglich ist. Man hat daher:

$$a_1 \cdot a_2 \ldots a_\lambda \cdot b_1 \cdot b_2 \ldots b_\mu = 1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2}$$

und

$$(-1)^\mu \cdot a_1 a_2 \ldots a_\lambda \cdot b_1 b_2 \ldots b_\mu \equiv 1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2} \cdot q^{\frac{p-1}{2}} \pmod{p}.$$

Da nun $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$ ist, so erhält man aus der Verbindung mit den beiden vorigen Relationen:

$$\left(\frac{q}{p}\right) \equiv (-1)^\mu \pmod{p}$$

*) Liouville sur la loi de réciprocité dans la théorie des résidus quadratiques, in seinem J. Bd. 12; Eisenstein, application de l'algèbre à l'arithmétique transcendante, in Crelle's J. Bd. 29.

oder vielmehr

$$\left(\frac{q}{p}\right) = (-1)^{\mu}.$$

Dies voraus geschickt, ist es leicht, einen Ausdruck aus Einheitswurzeln zu bilden, welcher gleich $\left(\frac{q}{p}\right)$ ist. In der That findet man:

$$(37) \qquad \left(\frac{q}{p}\right) = \prod_{\alpha=1}^{\alpha=\frac{p-1}{2}} \frac{r^{\alpha q} - r^{-\alpha q}}{r^{\alpha} - r^{-\alpha}},$$

da in dem Producte jedesmal ein Factor des Zählers einem Factor des Nenners gleich wird, sobald αq einer der Zahlen a, dagegen einem Factor des Nenners entgegengesetzt gleich wird, sobald αq einer der Zahlen $-b$ des Hilfssatzes (mod. p) congruent ist, sodass das ganze Product den Werth $(-1)^{\mu}$ erhält. Ist nun ϱ eine primitive Wurzel von $x^q = 1$, so ist ebenso:

$$(38) \qquad \left(\frac{p}{q}\right) = \prod_{\beta=1}^{\beta=\frac{q-1}{2}} \frac{\varrho^{\beta p} - \varrho^{-p\beta}}{\varrho^{\beta} - \varrho^{-\beta}}.$$

Dies sind, unter etwas anderer Form, die Ausdrücke, welche Eisenstein und Liouville bei ihren Beweisen benutzt haben. Im weiteren Verlaufe ist des Erstern Beweis dem Liouville-schen insofern vorzuziehen, als dieser weniger symmetrisch und direct verfährt. Jener schliesst das Reciprocitätsgesetz durch directe Vergleichung der beiden Ausdrücke von $\left(\frac{p}{q}\right)$ und $\left(\frac{q}{p}\right)$, welche etwa folgendermassen bewerkstelligt werden kann: Da

$$\frac{x^p - 1}{x - 1} = (x - r^2)(x - r^4) \dots (x - r^{2(p-1)})$$

gesetzt werden kann, so ergiebt sich für $x = \frac{a}{b}$:

$$\frac{a^p - b^p}{a - b} = \prod_{\alpha=1}^{\alpha=p-1} (a - b r^{2\alpha}) = \prod_{\alpha=1}^{\alpha=\frac{p-1}{2}} (a - b r^{2\alpha})(a - b r^{-2\alpha})$$

$$(39) \qquad = \prod_{\alpha=1}^{\alpha=\frac{p-1}{2}} (a r^{\alpha} - b r^{-\alpha})(a r^{-\alpha} - b r^{\alpha}),$$

und auf ähnlichem Wege:

$$(40) \qquad \frac{a^q - b^q}{a - b} = \prod_{\beta=1}^{\beta=\frac{q-1}{2}} (a\varrho^{\beta} - b\varrho^{-\beta})\,(a\varrho^{-\beta} - b\varrho^{\beta})\,.$$

Bezeichnet also R eine solche primitive Wurzel der Gleichung $x^{pq} = 1$, dass $r = R^q$, $\varrho = R^p$ ist, so findet sich, wenn in der Formel (39) $a = \varrho^{\beta}$, $b = \varrho^{-\beta}$ gesetzt wird:

$$\left(\frac{p}{q}\right) = \prod_{\alpha=1}^{\alpha=\frac{p-1}{2}} \prod_{\beta=1}^{\beta=\frac{q-1}{2}} (R^{\alpha q+\beta p} - R^{-\alpha q-\beta p})\,(R^{-\alpha q+\beta p} - R^{\alpha q-\beta p})$$

und, wenn in (40) $a = r^{\alpha}$, $b = r^{-\alpha}$ gesetzt wird:

$$\left(\frac{q}{p}\right) = \prod_{\alpha=1}^{\alpha=\frac{p-1}{2}} \prod_{\beta=1}^{\beta=\frac{q-1}{2}} (R^{\alpha q+\beta p} - R^{-\alpha q-\beta p})\,(R^{\alpha q-\beta b} - R^{-\alpha q+\beta p})\,.$$

In diesem Producte hat jedesmal der erste Factor gleichen, der zweite Factor entgegengesetzten Werth, wie im vorigen; da das Product im Ganzen aus $\frac{p-1}{2} \cdot \frac{q-1}{2}$ solchen Gliedern besteht, findet man also endlich

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}\,.$$

Liouville dagegen wendet die, aus der Formel (39) dadurch, dass $a = b = 1$ gesetzt wird, sich ergebende Gleichung

$$p = (-1)^{\frac{p-1}{2}} \cdot \prod_{\alpha=1}^{\alpha=\frac{p-1}{2}} (r^{\alpha} - r^{-\alpha})^2$$

und die Beziehung $p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right)$ (mod. q) an. Erhebt man nämlich die vorige Gleichung zur Potenz $\frac{q-1}{2}$, multiplicirt im Zähler und Nenner der rechten Seite mit $\prod_{\alpha=1}^{\alpha=\frac{p-1}{2}} (r^{\alpha} - r^{-\alpha})$ und lässt in der q^{ten} Potenz dieses Products, das dann den Zähler der rechten Seite bildet, alle durch q theilbaren Glieder fort, so nimmt die letztere Beziehung die Gestalt an:

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot \prod_{\alpha=1}^{\alpha=\frac{p-1}{2}} \frac{r^{\alpha q} - r^{-\alpha q}}{r^{\alpha} - r^{-\alpha}} \equiv \left(\frac{p}{q}\right) \pmod{q}$$

und ergiebt durch Vergleichung mit (37) das Reciprocitätsgesetz.

Ohne näher auf den 4ten Gaussischen Beweis hier eingehen zu können, wollen wir doch noch zum Schluss bemerken, dass auch er mit den beiden eben mitgetheilten Beweisen dem Princip nach identisch ist. In der That ist nach den Gleichungen (22) und (25)

$$S = \prod_{h=1}^{h=\frac{p-1}{2}} (r^{2h-1} - r^{-2h+1}),$$

wofür aber nach den Gleichungen (20) auch

$$S = \varepsilon_p \cdot \prod_{\alpha=1}^{\alpha=\frac{p-1}{2}} (r^{\alpha} - r^{-\alpha})$$

gesetzt werden kann, wenn ε_p gleich $(-1)^{\frac{p-1}{4}}$ oder gleich $(-1)^{\frac{p-3}{4}}$ genommen wird, jenachdem p von der Form $4n+1$ oder $4n+3$ ist. Bezeichnen wir nun S mit $\psi(1, p)$ und S_q mit $\psi(q, p)$, sodass

$$\psi(1, p) = \varepsilon_p \cdot \prod_{\alpha=1}^{\alpha=\frac{p-1}{2}} (r^{\alpha} - r^{-\alpha}), \quad \psi(q, p) = \varepsilon_p \cdot \prod_{\alpha=1}^{\alpha=\frac{p-1}{2}} (r^{\alpha q} - r^{-\alpha q})$$

ist, so betrachtet Gauss den Quotienten $\frac{\psi(q, p)}{\psi(1, p)}$, für welchen nach (19) die Gleichung $\left(\frac{q}{p}\right) = \frac{\psi(q, p)}{\psi(1, p)}$ besteht. Ebenso wird sein:

$$\left(\frac{p}{q}\right) = \frac{\psi(p, q)}{\psi(1, q)}$$

wenn gesetzt wird:

$$\psi(1, q) = \varepsilon_q \cdot \prod_{\beta=1}^{\beta=\frac{q-1}{2}} (\varrho^{\beta} - \varrho^{-\beta}), \quad \psi(p, q) = \varepsilon_q \cdot \prod_{\beta=1}^{\beta=\frac{q-1}{2}} (\varrho^{\beta p} - \varrho^{-\beta p})$$

$$\varepsilon_q = \begin{Bmatrix} (-1)^{\frac{q-1}{4}} \\ (-1)^{\frac{q-3}{4}} \end{Bmatrix}, \text{ wenn } \begin{cases} q = 4n+1 \\ q = 4n+3 \end{cases}.$$

Diese Gleichungen, aus welchen sich

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=\frac{\psi(p,q)\cdot\psi(q,p)}{\psi(1,q)\cdot\psi(1,p)}$$

ergiebt, sind dieselben, wie die Gleichungen (37) und (38), und der Unterschied des Gaussischen Beweises von den eben dargestellten besteht nur darin, dass der Werth des Quotienten auf der Rechten der letzten Gleichung, welcher vorher aus der Vergleichung der Factoren der ψ-Functionen gebildet wurde, bei Gauss aus den fertigen Werthen, welche er für die ψ-Functionen in seiner Abhandlung bestimmt hat, abgeleitet wird.

Zehnte Vorlesung.

Anwendung der Kreistheilung zur Zerlegung der Zahlen in Quadrate.

1. Bevor wir von den quadratischen Resten zur Betrachtung der Reste höherer Potenzen übergehen, ist es zweckmässig, eine andere Anwendung der Kreistheilung auf die Zahlentheorie, welche die Zerlegung der Zahlen in Quadrate betrifft, hier einzuschalten. Wir haben zu diesem Zwecke an die mit $\psi(h, k, \omega)$ bezeichnete Function wieder anzuknüpfen und zwei Eigenschaften derselben abzuleiten, welche für die meisten Anwendungen der Kreistheilung auf arithmetische Fragen die wesentlichste Grundlage bilden.

Es war aber

$$\psi(h, k, \omega)=\frac{(\omega^k, r).(\omega^h, r)}{(\omega^{h+k}, r)},$$

ein Ausdruck, welcher nach Gleichung (28) der 8. Vorlesung den Werth

$$(1)\qquad \psi(h, k, \omega)=\sum_{\mu=1}^{\mu=p-2}\omega^{h\,\mathrm{ind}.\,\mu-(h+k)\,\mathrm{ind}.\,(1+\mu)}$$

hat, wenn die Summe der Zahlen h, k nicht durch $p-1$ theilbar ist. Ersetzen wir hierin h, k durch $-h, -k$ und multipliciren die entstehende Gleichung mit der Gleichung (1), so er-

halten wir:

$$\frac{(\omega^h, r)(\omega^{-h}, r) \cdot (\omega^k, r)(\omega^{-k}, r)}{(\omega^{h+k}, r)(\omega^{-h-k}, r)}$$

$$= \sum_{\mu=1}^{\mu=p-2} \omega^{h \operatorname{ind.} \mu - (h+k) \operatorname{ind.} (1+\mu)} \cdot \sum_{\mu=1}^{\mu=p-2} \omega^{-h \operatorname{ind.} \mu + (h+k) \operatorname{ind.} (1+\mu)}.$$

Da nun, wenn auch h und k durch $p-1$ nicht theilbar sind, nach Gleichung (29) der 8. Vorlesung

$$(\omega^h, r)(\omega^{-h}, r) = (-1)^h \cdot p, \quad (\omega^k, r)(\omega^{-k}, r) = (-1)^k \cdot p$$
$$(\omega^{h+k}, r)(\omega^{-h-k}, r) = (-1)^{h+k} \cdot p$$

ist, so hat der Quotient auf der linken Seite den einfachen Werth p, und man erhält die wichtige Gleichung:

(2) $$p = \psi(h, k, \omega) \cdot \psi(p-1-h, p-1-k, \omega)$$

oder:

(3) $$p = \sum_{\mu=1}^{\mu=p-2} \omega^{h \operatorname{ind.} \mu - (h+k) \operatorname{ind.} (1+\mu)} \cdot \sum_{\mu=1}^{\mu=p-2} \omega^{-h \operatorname{ind.} \mu + (h+k) \operatorname{ind.} (1+\mu)}$$

d. i. **eine Zerlegung der Primzahl p in zwei, offenbar conjugirte, complexe ganze Zahlen**, welche je nach den verschiedenen Werthen, welche man h und k beilegen kann, aus Einheitswurzeln verschiedener Grade zusammengesetzt sein werden.

Nimmt man z. B. $k = nh$ an, so wird (s. Formel (30) der 8. Vorlesung)

(4) $$\psi(h, nh, \omega) = \psi_n(\omega^h),$$

und die Gleichungen (2) und (3) erhalten folgende Gestalt:

(5) $$p = \psi_n(\omega^h) \cdot \psi_n(\omega^{-h}),$$

und

(6) $$p = \sum_{\mu=1}^{\mu=p-2} (\omega^h)^{\operatorname{ind.} \mu - (n+1) \operatorname{ind.} (1+\mu)} \cdot \sum_{\mu=1}^{\mu=p-2} (\omega^h)^{- \operatorname{ind.} \mu + (n+1) \operatorname{ind.} (1+\mu)}.$$

Für $h = f$ darf $k = (e-2)f$ gewählt werden, und dadurch erhält man, indem man wieder ω^f mit α bezeichnet, vermittelst der Formel

(7) $$p = \sum_{\mu=1}^{\mu=p-2} \alpha^{\operatorname{ind.} \mu + \operatorname{ind.} (1+\mu)} \cdot \sum_{\mu=1}^{\mu=p-2} \alpha^{- \operatorname{ind.} \mu - \operatorname{ind.} (1+\mu)}$$

eine Zerlegung der Primzahl p in zwei conjugirte com-

so ergiebt sich:

$$\sum_{\mu=1}^{\mu=p-2} \alpha^{\text{ind.}\,\mu + \text{ind.}\,(1+\mu)} = 12 + 12\alpha + 6\alpha^2 + 15\alpha^3 + 14\alpha^4,$$

also

$$61 = (12+12\alpha+6\alpha^2+15\alpha^3+14\alpha^4)(12+12\alpha^4+6\alpha^3+15\alpha^2+14\alpha).$$

2. Wir bezeichnen hinfort mit $\psi\,(h, k, g)$ den Ausdruck, welcher aus $\psi\,(h, k, \omega)$ hervorgeht, wenn die primitive Wurzel ω der Gleichung $x^{p-1} = 1$ durch die primitive Wurzel g der Congruenz $x^{p-1} \equiv 1 \pmod{p}$ ersetzt wird. Für zwei Zahlen h, k, deren Summe durch $p - 1$ nicht theilbar ist, werden wir demnach haben:

$$\psi\,(h, k, g) = \sum_{\mu=1}^{\mu=p-2} g^{h\,\text{ind.}\,\mu - (h+k)\,\text{ind.}\,(1+\mu)}. \tag{10}$$

Indem wir nun h und k als positive Zahlen voraussetzen, welche kleiner als $p-1$ sind, unterscheiden wir zwei mögliche Fälle: entweder ist $h + k < p - 1$, und dann ist, wenn wir $n = p - 1 - h - k$ setzen, n ebenfalls kleiner als $p - 1$, ebenso auch $h + n = p - 1 - k$. Alsdann kann man setzen:

$$\psi(h, k, g) \equiv \sum_{\mu=1}^{\mu=p-2} g^{h\,\text{ind.}\,\mu + n\,\text{ind.}\,(1+\mu)} \pmod{p}$$

oder:

$$\psi\,(h, k, g) \equiv \sum_{\mu=1}^{\mu=p-1} \mu^h \,.\, (\mu + 1)^n \pmod{p},$$

indem man die Summation bis $\mu = p - 1$ erstrecken darf, weil das entsprechende Glied der Summe durch p theilbar wird. Denkt man sich die Potenz $(\mu + 1)^n$ nach dem binomischen Lehrsatze entwickelt, so nimmt diese Congruenz die Gestalt an:

$$\psi\,(h, k, g) \equiv \sum_1^{p-1} \mu^{h+n} + n_1 \sum_1^{p-1} \mu^{h+n-1} + \ldots + n_{n-1} \sum_1^{p-1} \mu^{h+1} + \sum_1^{p-1} \mu^h \pmod{p}, \tag{11}$$

in welcher $n_1, n_2, \ldots . n_{n-1}$ die Binomialcoëfficienten der n^{ten} Potenz bezeichnen.

Hier wollen wir nun bemerken, dass $\sum_1^{p-1} \mu^k$ entweder der Null oder der negativen Einheit (mod. p) congruent ist, Letzteres, wenn

k durch $p-1$ theilbar ist, nach dem Fermat'schen Lehrsatze, Ersteres, wenn k nicht durch $p-1$ theilbar ist, deshalb, weil dann

$$\sum_{\mu=1}^{\mu=p-1} \mu^k \equiv \sum_{\mu=1}^{\mu=p-1} g^{k\,\mathrm{ind}.\mu} \equiv \sum_{\lambda=0}^{\lambda=p-2} g^{k\lambda} \quad (\mathrm{mod.}\ p)$$

und die letzte Summe gleich $\frac{g^{k(p-1)}-1}{g^k-1}$, folglich der Null congruent ist.

Da nun $h+n<p-1$ ist, wird der Exponent in keiner der Summen, welche die Congruenz (11) enthält, durch $p-1$ theilbar, und daher

$$\psi(h, k, g) \equiv 0 \quad (\mathrm{mod.}\ p)$$

sein.

Oder es ist $h+k>p-1$, während es doch $<2(p-1)$ sein muss; setzt man dann $n=2(p-1)-h-k$, so wird $n<p-1$, aber $n+h=2(p-1)-k$ zwischen $p-1$ und $2(p-1)$ enthalten sein. Da jetzt wieder

$$\psi(h, k, g) \equiv \sum_{\mu=1}^{\mu=p-1} \mu^h (\mu+1)^n \quad (\mathrm{mod.}\ p)$$

gesetzt werden kann, und in den Summen, welche die daraus hervorgehende Congruenz (11) enthält, nur ein Exponent durch $p-1$ theilbar wird, nämlich derjenige $h+n-s$, welcher gleich $p-1$, oder für welchen $s=p-1-k$ ist, so wird nach der vorher gemachten Bemerkung

$$\psi(h, k, g) \equiv -n_{p-1-k} \quad (\mathrm{mod.}\ p).$$

Hiernach ergiebt sich der Satz: Jenachdem in der Function $\psi(h, k, g)$ die Summe der beiden Zahlen h und k kleiner oder grösser ist als $p-1$, während sie selbst kleiner als $p-1$ vorausgesetzt sind, ist

$$\left.\begin{array}{l} \psi(h, k, g) \equiv 0 \\ \text{oder} \\ \psi(h, k, g) \equiv -\dfrac{\Pi(2(p-1)-h-k)}{\Pi(p-1-h).\Pi(p-1-k)} \end{array}\right\} (\mathrm{mod.}\ p),$$

wo die Zeichen Π die Producte aller ganzen Zahlen bis zu den angedeuteten Zahlen hin bedeuten*)

*) S. Jacobi in der Note über Kreistheilung Cr. 7. Bd. 30; vgl. Eisenstein in seinem Beweise des cubischen Reciprocitätsgesetzes in Cr. J. Bd. 27.

3. Von diesen allgemeinen Betrachtungen, welche für das Folgende die Grundlage bilden, wollen wir nun zu einigen besonders interessanten speciellen Fällen übergehen.

Sei zuerst p von der Form $4n+1$, sodass $p-1$ den Factor 4 hat, den wir für e nehmen. Dann entspringt aus der Formel (7), wenn man beachtet, dass α als primitive vierte Einheitswurzel die imaginäre Zahl i ist, die folgende:

$$(12) \qquad p = \sum_{\mu=1}^{\mu=p-2} i^{\text{ind.}(\mu+\mu^2)} \cdot \sum_{\mu=1}^{\mu=p-2} i^{-\text{ind.}(\mu+\mu^2)}.$$

Unterscheiden wir die Fälle, in denen ind. $(\mu+\mu^2)$ einer der Zahlen 0, 1, 2, 3 (mod. 4) congruent ist, und bezeichnen mit A_0, A_1, A_2, A_3, wie oft jeder dieser Fälle sich ereignet, so wird

$$(13) \qquad A_0 + A_1 + A_2 + A_3 = p-2$$

und

$$(14) \qquad \sum_{\mu=1}^{\mu=p-2} i^{\text{ind.}(\mu+\mu^2)} = A_0 - A_2 + i\,(A_1 - A_3)$$

sein. Setzt man daher $A_0 - A_2 = a$, $A_1 - A_3 = b$, so ergiebt sich aus (12):

$$(15) \qquad p = a^2 + b^2,$$

d. h. der berühmte Satz der höheren Arithmetik: **Jede Primzahl von der Form $4n+1$ kann als Summe zweier Quadratzahlen dargestellt werden.**

Wenn so von diesem arithmetischen Satze ein einfacher Beweis aus der Kreistheilung gewonnen wird, liefert dieselbe noch den nicht zu unterschätzenden Vortheil, dass man die Werthe der ganzen Zahlen a, b nach der früher angegebenen Methode mit Leichtigkeit berechnen kann. Um ein Beispiel zu betrachten, sei $p = 13$. Nimmt man $g = 6$ als primitive Wurzel, so erhält man:

$$\begin{array}{rl} \mu = & 1,\ 2,\ 3,\ 4,\ 5, 6,\ 7, 8, 9, 10, 11, 12 \\ \text{ind.}\,\mu = & 0,\ 5,\ 8, 10,\ 9, 1,\ 7, 3, 4,\ 2, 11,\ 6 \\ \text{ind.}\,\mu' + \text{ind.}\,(1+\mu) = & 5, 13, 18, 19, 10, 8, 10, 7, 6, 13, 17, \\ \text{ind.}\,\mu + \text{ind.}\,(1+\mu) \equiv & 1,\ 1,\ 2,\ 3,\ 2, 0,\ 2, 3, 2,\ 1,\ 1 \ (\text{mod. } 4) \end{array}$$

also:

$$\sum_{\mu=1}^{\mu=11} i^{\text{ind.}(\mu+\mu^2)} = 1 + 4i + 4i^2 + 2i^3 = -3 + 2i,$$

$$a = -3,\ b = 2$$

und:

$$13 = 3^2 + 2^2.$$

Ein zweites Beispiel sei $p = 17$. Für die primitive Wurzel $g = 3$ findet man:

$$\begin{array}{rl} \mu = & 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11, \\ & 12,\ 13,\ 14,\ 15,\ 16 \\ \text{ind.}\,\mu = & 0,\ 14,\ 1,\ 12,\ 5,\ 15,\ 11,\ 10,\ 2,\ 3,\ 7, \\ & 13,\ 4,\ 9,\ 6,\ 8 \\ \text{ind.}\,\mu + \text{ind.}\,(1+\mu) = & 14,\ 15,\ 13,\ 17,\ 20,\ 26,\ 21,\ 12,\ 5,\ 10,\ 20, \\ & 17,\ 13,\ 15,\ 14 \\ \text{ind.}\,\mu + \text{ind.}\,(1+\mu) \equiv & 2,\ 3,\ 1,\ 1,\ 0,\ 2,\ 1,\ 0,\ 1,\ 2,\ 0, \\ & 1,\ 1,\ 3,\ 2\ (\text{mod. } 4). \end{array}$$

Daher ergiebt sich:

$$\sum_{\mu=1}^{\mu=15} i^{\text{ind.}(\mu+\mu^2)} = 3 + 6i + 4i^2 + 2i^3 = -1 + 4i,$$

$$a = -1,\ b = 4$$

und

$$17 = 1^2 + 4^2.$$

4. In der Zerlegung

$$p = x^2 + y^2$$

einer Primzahl p von der Form $4n + 1$ muss eins der Quadrate nothwendig gerade, das andere ungerade sein. Es besteht nun der Satz, dass eine solche Zerlegung eine völlig bestimmte ist, oder dass es nur eine einzige Zerlegung dieser Art giebt. Hiervon wird später ein aus allgemeineren Principien geschöpfter Beweis gegeben werden, hier mag der folgende seiner Einfachheit wegen Platz finden. Angenommen, man habe auch noch

$$p = \xi^2 + \eta^2,$$

und x^2, ξ^2 seien die ungeraden, y^2, η^2 die geraden Quadrate beider Zerlegungen, so ist leicht zu sehen, dass $\xi^2 = x^2$, $\eta^2 = y^2$ sein muss. Denn aus den beiden Zerlegungen folgen die drei Gleichungen:

$$p^2 = (x\xi + y\eta)^2 + (x\eta - y\xi)^2,\quad p^2 = (x\xi - y\eta)^2 + (x\eta + y\xi)^2$$
$$p(\eta^2 - y^2) = (x\eta + y\xi)(x\eta - y\xi);$$

da wegen der letztern einer der Factoren $x\eta + y\xi$, $x\eta - y\xi$

durch p theilbar, wegen der beiden erstern jeder derselben aber offenbar kleiner als p sein muss, so muss einer von ihnen gleich Null sein, was sofort die beiden Gleichungen $\eta^2 = y^2$, also $\xi^2 = x^2$ zur Folge hat.

Wird nun aber auf irgend einem Wege p als die Summe zweier Quadratzahlen:

$$p = x^2 + y^2$$

gefunden, so entsteht die Frage, welches der beiden Quadrate das gerade, welches das ungerade sei, und, da zwei Zahlen von gleichem Werthe, aber entgegengesetzten Vorzeichen dasselbe Quadrat haben, bleibt ferner zu untersuchen, ob die Zahlen x, y positiv oder negativ sind. Wir wollen diese Untersuchung für die durch die Formeln der Kreistheilung erhaltene Zerlegung

$$p = a^2 + b^2$$

hier durchzuführen suchen.

Es ist aber zunächst leicht zu sehen, dass dabei a die ungerade, b die gerade Zahl ist. Wir beginnen damit, die Summe

$$\sum_{\mu=1}^{\mu=p-2} i^{\text{ind.}\,\mu + \text{ind.}\,(1+\mu)}$$

zu transformiren. Setzen wir in den Formeln (29) und (30) der 8. Vorlesung $h = \frac{p-1}{4}$ und in der letzten sodann einmal $n = 1$, das andere Mal $n = 2$, so erhalten wir, da $\omega^{\frac{p-1}{4}} = i$, $\omega^{-\frac{p-1}{4}} = -i$ ist,

$$(16) \qquad (i, r) \,.\, (-i, r) = (-1)^{\frac{p-1}{4}} \,.\, p$$

$$(17) \qquad \psi_1(i) = \frac{(i, r)^2}{(-1, r)}, \quad \psi_2(i) = \frac{(i, r)\,(-1, r)}{(-i, r)}.$$

Die letzte dieser Formeln kann man auch folgendermassen schreiben:

$$(18) \qquad \psi_2(i) = \psi_1(i) \cdot \frac{(-1, r)^2}{(i, r)\,(-i, r)}.$$

Nun haben wir in Nr. 3 der vorigen Vorlesung gefunden, dass der Werth des Symbols $(-1, r)^2$ gleich $(-1)^{\frac{p-1}{2}} p = p$ ist, da hier $\frac{p-1}{2}$ gerade vorausgesetzt ist; wenn man daher die Gleichung (16) berücksichtigt, so nimmt die letzte Gleichung folgende Gestalt an:

$$(19) \qquad \psi_2(i) = (-1)^{\frac{p-1}{4}} \psi_1(i)$$

und giebt, wenn man für $\psi_1(i)$, $\psi_2(i)$ ihre Ausdrücke nach Gleichung (28) der vorletzten Vorlesung setzt, die bezweckte Transformation:

$$(20) \qquad \sum_{\mu=1}^{\mu=p-2} i^{\text{ind.}\mu+\text{ind.}(1+\mu)} = (-1)^{\frac{p-1}{4}} \cdot \sum_{\mu=1}^{\mu=p-2} i^{\text{ind.}\mu+2\,\text{ind.}(1+\mu)} \cdot$$

Aus dieser Gleichung, in welcher die linke Seite in der vorigen Nr. gleich $a + bi$ gesetzt worden ist, folgt nun zunächst, mit Vernachlässigung von Gliedern, welche den Coëfficienten 2 haben, die Congruenz:

$$a + b\,i \equiv \sum_{\mu=1}^{\mu=p-2} i^{\text{ind.}\mu} \pmod{2},$$

denn, da $i^{\text{ind.}\mu+2\,\text{ind.}(1+\mu)}$ entweder gleich $i^{\text{ind.}\mu}$ oder gleich $-\,i^{\text{ind.}\mu}$ ist, kann man allgemein

$$i^{\text{ind.}\mu+2\,\text{ind.}(1+\mu)} = i^{\text{ind.}\mu} + 2\,\varepsilon \cdot i^{\text{ind.}\mu}.$$

setzen, worin ε die Null oder die negative Einheit bedeutet, je nach den beiden möglichen Fällen. Nun befinden sich in der Reihe 1, 2, 3,... $p - 2$ nur $\frac{p-3}{2}$ quadratische Reste, weil -1 also auch $p-1$ quadratischer Rest von $p = 4n + 1$ ist, (nach Gleichung (7) der vorigen Vorlesung), die übrigen $\frac{p-1}{2}$ Zahlen sind quadratische Nichtreste, der Index von jenen ist eine gerade, der Index von diesen eine ungerade Zahl (nach Nr. 2 ebendaselbst), also findet man leicht:

$$a + bi \equiv \frac{p-3}{2} + i \cdot \frac{p-1}{2} \equiv 1 \pmod{2},$$

woraus a als die ungerade, b als die gerade Zahl sich ergiebt.

5. Es kann aber sogar noch weiter festgestellt werden, welchen der Reste $+1$ oder -1 die Zahl a, durch 4 getheilt, lässt. Setzen wir zu diesem Zwecke die Summe

$$\sum_{\mu=1}^{\mu=p-2} i^{\text{ind.}\mu+2\,\text{ind.}(1+\mu)}$$

in die Form:

$$\sum i^{\lambda+2k},$$

sodass

$$\lambda = \text{ind.}\,\mu\,,\ k = \text{ind.}\,(1+\mu)$$

ist, so muss diese neue Summe über alle Werthe von λ aus der Reihe $0, 1, 2, \ldots . p-2$ bezogen werden, den einen Werth $\frac{p-1}{2}$ ausgenommen, welchem $\mu = p-1$ d. i. ein Werth entsprechen würde, der in der ersten Summe nicht mehr zu nehmen war; jedem Werthe von λ entsprechend ist k so zu bestimmen, dass die Congruenz

$$g^k \equiv 1 + g^\lambda \pmod{p}$$

erfüllt wird. Wenn nun

$$\sum i^{\lambda+2k} = \alpha + \beta i$$

gesetzt wird, so findet man α, wenn man λ nur die geradzahligen Werthe annehmen lässt, welche ihm zukommen, es wird also:

$$\alpha = \sum (-1)^{\lambda'+k}, \tag{21}$$

wenn man λ' alle Werthe $0, 1, 2, \ldots . \frac{p-3}{2}$ beilegt, mit Ausnahme von $\frac{p-1}{4}$, und k jedesmal durch die Congruenz

$$g^k \equiv 1 + g^{2\lambda'} \pmod{p} \tag{22}$$

bestimmt. Sieht man zunächst von dem Werthe $\lambda' = 0$ ab, so lassen sich die übrigen zulässigen Werthe in Paare ordnen von der Art, dass die Werthe eines Paares λ' und $\frac{p-1}{2} - \lambda'$ sind, und λ' die Werthe $1, 2, 3, \ldots . \frac{p-5}{4}$ anzunehmen hat. Sind k^0 und k' die zu einem Paare gehörigen Werthe von k, so findet man

$$g^{k^0+k'} \equiv (1+g^{2\lambda'})(1+g^{-2\lambda'}) \equiv g^{-2\lambda'}(1+g^{2\lambda'})^2 \pmod{p}$$

d. h. $g^{k^0+k'}$ ist einem Quadrate (mod. p) congruent, folglich $k^0 + k'$ eine gerade Zahl oder $k^0 \equiv k' \pmod{2}$. Für $\lambda' = 0$ liefert die Congruenz (22) $g^k \equiv 2 \pmod{p}$; nun ist (siehe weiter unten in Nr. 3 der 15. Vorlesung) Zwei quadratischer Rest oder Nichtrest von p, mit andern Worten: k gerade oder ungerade, jenachdem p die Form $8n+1$ oder $8n+5$ hat; das entsprechende Glied der Summe (21) kann also durch $(-1)^{\frac{p-1}{4}}$

ausgedrückt werden. Fasst man von den übrigen immer die beiden Glieder

$$(-1)^{\lambda'+k^0}, \; (-1)^{\frac{p-1}{2}-\lambda'+k'}$$

zusammen, welche einem der bezeichneten Werthepaare von λ' entsprechen, und welche gleichen Werth haben, da $\frac{p-1}{2}$ gerade, λ' aber mit $-\lambda'$, k^0 mit k' gleichartig, nämlich gleichzeitig gerade oder ungerade ist, so ergiebt sich:

$$\alpha = (-1)^{\frac{p-1}{4}} + 2 \, . \sum (-1)^{\lambda'+k}$$

wenn jetzt die Summe über alle Werthe $\lambda' = 1, 2, 3, \ldots . \frac{p-5}{4}$ erstreckt wird. Offenbar kann man daher, wenn mit A die Anzahl bezeichnet wird, welche angiebt, wie oft $\lambda' + k$ eine ungerade Zahl wird, jetzt

$$\alpha = (-1)^{\frac{p-1}{4}} + 2 \, . \frac{p-5}{4} - 4A$$

setzen. Diese Gleichung, als Congruenz (mod. 4) aufgefasst, liefert in beiden Fällen, für $p = 8n + 1$ wie für $p = 8n + 5$, dasselbe Resultat, nämlich:

$$\alpha \equiv -1 \pmod{4} .$$

Daher erhält man aus Gleichung (20):

$$a \equiv -(-1)^{\frac{p-1}{4}} \pmod{4}$$

d. h. a ist von der Form $4n - 1$, wenn $p \equiv 1 \pmod{8}$, von der Form $4n + 1$, wenn $p \equiv 5 \pmod{8}$ ist, wie es an den beiden in Nr. 3 gegebenen Beispielen sich bestätigt.

6. Durch diese Betrachtungen wird a priori über die Frage entschieden, mit welchem Vorzeichen behaftet die Basis des ungeraden Quadrates in der Zerlegung von p durch die Methode der Kreistheilung erhalten wird. Bezeichnet nämlich $p = A + B$ die völlig bestimmte Zerlegung von p als Summe einer ungeraden Quadratzahl A und einer geraden Quadratzahl B, und α die positive Basis der erstern, so wird man, um daraus a zu erhalten, diese mit einem solchen Vorzeichen nehmen müssen, dass sie die Form $4n - 1$ oder $4n + 1$ annimmt, je nachdem p von der Form $8n + 1$ oder $8n + 5$ ist.

Z. B. ist $37 = 1 + 36$; da 37 die Form $8n + 5$ hat, wird die Kreistheilung die Zerlegung $37 = a^2 + b^2$ liefern, in welcher $a = +1$ ist.

Ferner ist $41 = 25 + 16$ und von der Form $8n + 1$, also wird man aus der Kreistheilung die Zerlegung $41 = a^2 + b^2$ finden, worin $a = -5$ ist.

Ueber das Vorzeichen von b kann ohne Weiteres, der Natur der Sache nach, nicht entschieden werden, da dasselbe von der willkürlichen Wahl der primitiven Wurzel g, auf welche in den obigen Summen die Indices bezogen sind, in der Art abhängt, dass es in das entgegengesetzte übergeht, wenn man g durch eine passende andere primitive Wurzel ersetzt. Um dies in der einfachsten Weise zu übersehen, wollen wir in dem Ausdrucke $\psi(h, k, g)$ der Nr. 2 $h = \frac{p-1}{4}$, $k = \frac{p-1}{2}$ setzen, wodurch

$$\psi\left(\frac{p-1}{4}, \frac{p-1}{2}, g\right) \equiv \sum_{\mu=1}^{\mu=p-2} \left(g^{\frac{p-1}{4}}\right)^{\text{ind.}(\mu+\mu^2)} \pmod{p}$$

wird. Da aber $g^{k.\frac{p-1}{4}}$ resp. den Zahlen $1, g^{\frac{p-1}{4}}, -1, -g^{\frac{p-1}{4}}$ (mod. p) congruent wird, jenachdem $k \equiv 0, 1, 2, 3$ (mod. 4) ist, so ergiebt sich offenbar.

$$\psi\left(\frac{p-1}{4}, \frac{p-1}{2}, g\right) \equiv A_0 + A_1 g^{\frac{p-1}{4}} - A_2 - A_3 g^{\frac{p-1}{4}}$$

oder

$$\psi\left(\frac{p-1}{4}, \frac{p-1}{2}, g\right) \equiv a + b\, g^{\frac{p-1}{4}} \pmod{p},$$

wenn A_0, A_1, A_2, A_3, a, b dieselben Zahlen bedeuten, wie in Nr. 3. Andererseits ist nach dem Satze in Nr. 2 $\psi\left(\frac{p-1}{4}, \frac{p-1}{2}, g\right) \equiv 0$ (mod. p), da $\frac{p-1}{4} + \frac{p-1}{2} < p - 1$ ist, demnach ergiebt sich

$$a + b g^{\frac{p-1}{4}} \equiv 0 \pmod{p}. \tag{23}$$

Hieraus erhellt jene Abhängigkeit; die, von g verschiedenen primitiven Wurzeln γ zerfallen nämlich in zwei Klassen, für deren eine $\gamma \equiv g^{4n+1}$ ist, während die andere der Congruenz $\gamma \equiv g^{4n+3}$

(mod. p) genügen. In der That, wenn g^λ eine primitive Wurzel ist, so ist $g^{-\lambda} = g^{p-1-\lambda}$ offenbar auch eine, von den beiden Zahlen λ und $p-1-\lambda$ aber ist eine stets von der Form $4n+1$, die andere von der Form $4n+3$. — Jenach diesen beiden Arten primitiver Wurzeln wird aber die Congruenz (23), wenn man g durch γ ersetzt, übergehen in:

$$a + b\gamma^{\frac{p-1}{4}} \equiv 0$$

oder in:

$$a - b\gamma^{\frac{p-1}{4}} \equiv 0\,.$$

7. Die Congruenz (23) dient aber nicht allein dazu, das Vorzeichen von b, sondern auch dazu, in Verbindung mit einer andern ähnlichen Congruenz die Zahlen a, b selbst zu bestimmen. Setzt man nämlich in dem allgemeinen Ausdrucke für $\psi\,(h, k, g)$ jetzt $h = 3\,.\,\frac{p-1}{4}$, $k = \frac{p-1}{2}$, so kommt:

$$\psi\left(3\,.\,\frac{p-1}{4}, \frac{p-1}{2}, g\right) \equiv \sum_{\mu=1}^{\mu=p-2} \left(g^{3\,.\,\frac{p-1}{4}}\right)^{\text{ind.}\,(\mu+\mu^2)}$$

$$\equiv a - b g^{\frac{p-1}{4}} \text{ (mod. } p);$$

andererseits wird nach dem Satze der Nr. 2, da $h + k = 5\,.\,\frac{p-1}{4}$ also $> p-1$ ist,

$$\psi\left(3\,.\,\frac{p-1}{4}, \frac{p-1}{2}, g\right) \equiv -\frac{\Pi\left(3\,.\,\frac{p-1}{4}\right)}{\Pi\left(\frac{p-1}{4}\right)\cdot\Pi\left(\frac{p-1}{2}\right)}$$

$$\equiv -\frac{\frac{p+1}{2}\,\ldots\,3\,.\,\frac{p-1}{4}}{1\,.\,2\,.\,3\,\ldots\,\frac{p-1}{4}} \text{ (mod. } p)$$

sein. Da

$$\frac{p+1}{2} \equiv -\frac{p-1}{2},\ \frac{p+3}{2} \equiv -\frac{p-3}{2},\ \ldots\ 3\,.\frac{p-1}{4} \equiv -\frac{p+3}{4} \text{ (mod. } p),$$

so lässt sich die rechte Seite dieser Congruenz auch auf die Form bringen:

$$-(-1)^{\frac{p-1}{4}} \frac{\Pi\left(\frac{p-1}{2}\right)}{\left(\Pi\frac{p-1}{4}\right)^2},$$

sodass man findet:

$$(24) \qquad a - bg^{\frac{p-1}{4}} \equiv (-1)^{\frac{p+3}{4}} \frac{\Pi\left(\frac{p-1}{2}\right)}{\left(\Pi\frac{p-1}{4}\right)^2} \text{ mod. } p).$$

Aus den beiden Formeln (23) und (24) ergiebt sich durch Addition:

$$(25) \qquad a \equiv (-1)^{\frac{p+3}{4}} \cdot \tfrac{1}{2} \frac{\Pi\left(\frac{p-1}{2}\right)}{\left(\Pi\frac{p-1}{4}\right)^2} \text{ (mod. } p)$$

und durch Subtraction:

$$(26) \qquad b \cdot g^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{4}} \cdot \tfrac{1}{2} \frac{\Pi\left(\frac{p-1}{2}\right)}{\left(\Pi\frac{p-1}{4}\right)^2} \text{ (mod. } p) \,.$$

Hier kann man noch bemerken, dass aus Wilson's Satze:

$$1 \cdot 2 \cdot 3 \ldots\ldots (p-1) \equiv -1 \text{ (mod. } p)$$

und den Congruenzen:

$$p - 1 \equiv -1, p - 2 \equiv -2, \ldots\ldots \frac{p+1}{2} \equiv -\frac{p-1}{2} \text{ mod. } p),$$

da $\frac{p-1}{2}$ gerade und $g^{\frac{p-1}{2}} \equiv -1$ (mod. p) ist, sich die folgende Beziehung:

$$\left(1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2}\right)^2 \equiv g^{\frac{p-1}{2}},$$

also

$$(27) \qquad 1 \cdot 2 \cdot 3 \ldots\ldots \frac{p-1}{2} \equiv \pm g^{\frac{p-1}{4}} \text{ (mod. } p)$$

ableiten lässt, in welcher das positive oder negative Vorzeichen der Wahl von g gemäss genommen werden muss. Wendet man diese Beziehung an, so findet man aus (26):

$$(28) \qquad \pm 2b \cdot \left(\Pi \frac{p-1}{4}\right)^2 \equiv (-1)^{\frac{p-1}{4}} \text{ (mod. } p),$$

wo das Vorzeichen dem Vorzeichen in (27) correspondirt.

Die beiden Formeln (25) und (28) sind sehr interessant, weil sie lehren, eine Zerfällung der Primzahl p in die Summe zweier Quadrate direct zu bestimmen. In der That, durch diese Formeln sind nicht allein die Reste von a, b (mod. p), sondern

diese Zahlen selbst vollkommen bestimmt. — Es ergiebt sich nämlich leicht aus der Formel $p = a^2 + b^2$, dass a und b den absoluten Werth $\frac{p-1}{2}$ nicht übersteigen dürfen. Denn $a^2 = p - b^2$ ist $< p - 1$; wäre aber $a = \pm \left(\frac{p-1}{2} + a'\right)$, während a' positiv ist, so ergäbe sich $a^2 > p - 1$, und ähnlich ist es mit b. Hieraus folgt, dass a, b die absolut kleinsten, zwischen $-\frac{p-1}{2}$ und $+\frac{p-1}{2}$ enthaltenen Reste sind, welche den Congruenzen (25) und (28) Genüge leisten.

Wir fassen die letzten Resultate in folgenden Satz zusammen: **Bestimmt man die Zahlen a, b als die absolut kleinsten Reste, welche den Congruenzen**

$$a \equiv (-1)^{\frac{p+3}{4}} \cdot \frac{1}{2} \frac{\Pi\left(\frac{p-1}{2}\right)}{\left(\Pi \frac{p-1}{4}\right)^2}, \quad \pm 2b \cdot \left(\Pi \frac{p-1}{4}\right)^2 \equiv (-1)^{\frac{p-1}{4}} \pmod{p}$$

Genüge leisten, so erhält man unmittelbar die Zerlegung von p in die Summe zweier Quadratzahlen, nämlich

$$p = a^2 + b^2 .$$

Dieser Satz, in ein wenig anderer Gestalt, ist zuerst von **Gauss** in seiner ersten Abhandlung über die biquadratischen Reste*) angegeben worden. Er bemerkt daselbst noch, dass, während über das Vorzeichen von a in der vorher ausgeführten Art entschieden werden kann, ein ähnliches Criterium zur Bestimmung des Vorzeichens für die Basis des geraden Quadrates ihm nicht bekannt sei. Während ein solches auch bis jetzt, soviel ich weiss, nicht für jeden Fall aufgefunden ist, werden wir auf ein, für den Fall $p = 8n + 5$ von **Stern** angegebenes Criterium bei einer späteren Gelegenheit zurückzukommen haben.

---

*) **Gauss**, theoria residuorum biquadraticorum commentatio prima, in seinen Werken Bd. II. Derselbe Satz findet sich auch bewiesen in **Cauchy's** mém. sur la théorie des nombres pag. 728, sowie in **Lebesgue**, recherches sur les nombres, in **Liouv.** J. Bd. 2 pag. 283.

Elfte Vorlesung.

Fortsetzung: Die Fälle $p = 6n + 1$ und $p = 8n + 1$.

1. Wir setzen, um eine zweite Anwendung der in der vor. Vorl. entwickelten Principien zu machen, p von der Form $6n + 1$ voraus, sodass $p - 1$ den Factor 3 hat, der jetzt für e genommen werden soll. Dann liefert die Formel (7) die folgende:

$$(1) \qquad p = \sum_{\mu=1}^{\mu=p-2} \varrho^{\text{ind.}(\mu+\mu^2)} \cdot \sum_{\mu=1}^{\mu=p-2} \varrho^{-\text{ind.}(\mu+\mu^2)},$$

wenn man mit ϱ eine imaginäre cubische Einheitswurzel bezeichnet. Die beiden Summen sind resp. gleich

$$A_0 + A_1\varrho + A_2\varrho^2 \text{ und } A_0 + A_1\varrho^2 + A_2\varrho,$$

wo A_0, A_1, A_2 die Anzahl bezeichnen, wie oft ind. $(\mu + \mu^2)$ einer der Zahlen 0, 1, 2 resp. (mod. 3) congruent ist, sodass die Gleichung besteht:

$$(2) \qquad A_0 + A_1 + A_2 = p - 2\,.$$

Da aber ϱ die Gleichung $1 + \varrho + \varrho^2 = 0$ befriedigt, kann man die Summen in der vorigen Zerlegung auch auf die Form

$$a + b\varrho \text{ und } a + b\varrho^2$$

bringen, worin a, b wieder ganze Zahlen, nämlich

$$(3) \qquad a = A_0 - A_2,\; b = A_1 - A_2$$

sind, und da das Product jener Werthe nach der Gleichung $1 + \varrho + \varrho^2 = 0$ die Form $a^2 - ab + b^2$ annimmt, so erhält man wieder einen interessanten Satz der höheren Arithmetik: Jede Primzahl von der Form $6n + 1$ kann in die Form $a^2 - ab + b^2$ gesetzt werden.

Derselbe kann noch in einer etwas verschiedenen Gestalt ausgesprochen werden. Da nämlich $\varrho = \frac{-1+\sqrt{-3}}{2}, \varrho^2 = \frac{-1-\sqrt{-3}}{2}$ gewählt werden darf, so gehen die Ausdrücke $a + b\varrho$, $a + b\varrho^2$ in $\frac{A + B\sqrt{-3}}{2}$, $\frac{A - B\sqrt{-3}}{2}$ resp. über, wenn

$$(4) \qquad A = 2a - b,\; B = b$$

gesetzt wird, und aus (1) folgt die Gleichung:

$$4p = A^2 + 3B^2, \tag{5}$$

d. h. der Satz: Das Vierfache jeder (ungeraden) Primzahl von der Form $6n+1$ kann als Summe aus einem einfachen und einem dreifachen Quadrate dargestellt werden.

Nehmen wir wieder als Beispiel $p = 13$. In diesem Falle findet man:

$$\mu = 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12$$

$$\text{ind.}\,\mu = 0,\ 5,\ 8,\ 10,\ 9,\ 1,\ 7,\ 3,\ 4,\ 2,\ 11,\ 6$$

$$\text{ind.}\,(\mu+\mu^2) = 5,\ 13,\ 18,\ 19,\ 10,\ 8,\ 10,\ 7,\ 6,\ 13,\ 17$$

$$\text{ind.}\,(\mu+\mu^2) \equiv 2,\ 1,\ 0,\ 1,\ 1,\ 2,\ 1,\ 1,\ 0,\ 1,\ 2 \pmod{3},$$

also

$$\sum_{\mu=1}^{\mu=11} \varrho^{\text{ind.}(\mu+\mu^2)} = 2 + 6\varrho + 3\varrho^2 = -1 + 3\varrho,$$

$$a = -1,\ b = 3,\ A = -5,\ B = 3$$

und die Zerlegungen:

$$13 = 1^2 + 1\,.\,3 + 3^2,\ 4\,.\,13 = 5^2 + 3\,.\,3^2.$$

Wird zweitens $p = 19$ gewählt, so wird gefunden, wenn für die primitive Wurzel g die 2 genommen wird:

$$\mu = 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15,\ 16,\ 17,\ 18$$

$$\text{ind.}\,\mu = 0,\ 1,\ 13,\ 2,\ 16,\ 14,\ 6,\ 3,\ 8,\ 17,\ 12,\ 15,\ 5,\ 7,\ 11,\ 4,\ 10,\ 9$$

$$\text{ind.}\,(\mu+\mu^2) = 1,\ 14,\ 15,\ 18,\ 30,\ 20,\ 9,\ 11,\ 25,\ 29,\ 27,\ 20,\ 12,\ 18,\ 15,\ 14,\ 19$$

$$\text{ind.}\,(\mu+\mu^2) \equiv 1,\ 2,\ 0,\ 0,\ 0,\ 2,\ 0,\ 2,\ 1,\ 2,\ 0,\ 2,\ 0,\ 0,\ 0,\ 2,\ 1 \pmod{3},$$

also

$$\sum_{\mu=1}^{\mu=17} \varrho^{\text{ind.}(\mu+\mu^2)} = 8 + 3\varrho + 6\varrho^2 = 2 - 3\varrho,$$

$$a = 2,\ b = -3,\ A = 7,\ B = -3$$

und die Zerlegungen:

$$19 = 2^2 + 2\,.\,3 + 3^2,\ 4\,.\,19 = 7^2 + 3\,.\,3^2.$$

2. Um zu untersuchen, welchen Rest die Zahl a (mod. 3) lässt, gehen wir aus von der Gleichung:

$$(\omega^h, r) = \sum_{\mu=1}^{\mu=p-1} \omega^{h\,\text{ind.}\mu}\,.\,r^\mu$$

und setzen darin successive $h = \frac{p-1}{3}$, wodurch $\omega^h = \varrho$ wird, und $h = 2 \, . \, \frac{p-1}{3}$, so entstehen die beiden Gleichungen:

(6) $$(\varrho, r) = \sum_{\mu=1}^{\mu=p-1} \varrho^{\text{ind.}\mu} \, . \, r^\mu, \quad (\varrho^2, r) = \sum_{\mu=1}^{\mu=p-1} \varrho^{2\,\text{ind.}\mu} \, . \, r^\mu.$$

Ferner findet man aus Gleichung (34) der 8. Vorlesung für $e = 3$, $f = \frac{p-1}{3}$ und $\alpha = \varrho$ folgendes Resultat:

$$(\varrho, r)^3 = (-1)^{\frac{p-1}{3}} \, . \, p \, \psi_1 \, (\varrho),$$

oder vielmehr, da $\frac{p-1}{3}$ gerade ist,

$$(\varrho, r)^3 = p \, . \, \psi_1 \, (\varrho),$$

während bei der Voraussetzung $h = \frac{p-1}{3}$ aus den Formeln (28) und (30) ebendaselbst

$$\psi_1 \, (\varrho) = \sum_{\mu=1}^{\mu=p-2} \varrho^{\text{ind.}\mu - 2\,\text{ind.}(1+\mu)} = \sum_{\mu=1}^{\mu=p-2} \varrho^{\text{ind.}(\mu+\mu^2)}$$

hervorgeht. Die vorletzte Gleichung kann demnach auch so geschrieben werden:

(7) $$(\varrho, r)^3 = p \, (a + b\varrho),$$

wenn a, b dieselben Zahlen bezeichnen, wie zuvor.

Endlich giebt die Gleichung (29) der 8. Vorlesung unter derselben Voraussetzung die Relation:

(8) $$(\varrho, r) \, . \, (\varrho^2, r) = (-1)^{\frac{p-1}{3}} \, . \, p,$$

aus welcher man mit Rücksicht auf (7) und, da

$$p = (a + b\varrho) \, (a + b\varrho^2)$$

gefunden worden ist,

(9) $$(\varrho^2, r)^3 = p \, (a + b\varrho^2)$$

erhält.

Nun liefert die Erhebung der ersten der Gleichungen (6) zum Cubus folgende Gleichung:

$$(\varrho, r)^3 = \sum_{\mu=1}^{\mu=p-1} \varrho^{3\,\text{ind.}\mu} \, . \, r^{3\mu} + 3 \, . \, W,$$

in welcher W eine ganze Function von r mit ganzzahligen com-

plexen Coëfficienten [illegible] der Form $x - \lambda y$ ist also gleich $U + \varrho V$ gesetzt werden kann, wenn U, V solche Functionen mit reellen Coëfficienten bedeuten. Da nun $\varrho^3 = 1$ und $\sum\limits_{k=1}^{k=p-1} r^k = -1$ ist, ergiebt sich mit Rücksicht auf [illegible].

(10) $\qquad p(x - \lambda y) - 1 = [\text{illegible}]\ V\varrho.$

In dieser Gleichung darf ϱ durch ϱ^2 ersetzt werden, da die entstehende Gleichung:

(11) $\qquad p(x - \lambda y) - 1 = [\text{illegible}]\ V\varrho^2$

aus der Erhebung von [illegible] zum Cubus in ähnlicher Weise abgeleitet werden kann. Durch ihre Verbindung mit der vorigen findet man aber die Gleichungen:

$$px + 1\ [\text{illegible}] \quad \text{also} \quad px + 1 = 2U,$$
$$pb\varrho\ (1 - \varrho) = [\text{illegible}] \quad \text{also} \quad py = 2V$$

aus denen man, weil sie [illegible] nur ganze reelle Zahlen enthalten, wegen der Irreductibilität der Kreistheilungsgleichung die Congruenzen

$$px - 1 \equiv [\text{illegible}] \quad py \equiv [\text{illegible}] \pmod{2},$$

folglich auch, da p [illegible] mod 2 ist, die folgenden

$$x \equiv -1 \quad [\text{illegible}] \pmod{2}$$

erschliesst*.

3. Auch hier kann, wie bei der Zerlegung der Primzahlen in die Summe zweier Quadrate gezeigt worden ist, die Zerlegung der Primzahlen p von der Form $6n + 1$ in complexe Factoren von der Form $a - \lambda b$ oder ihre Darstellung in der Form $a^2 - ab + b^2$ oder endlich was auf dasselbe hinauskommt, die Darstellung von $4p$ in der Form $A^2 + 27B^2$ durch geschlossene Formeln direct bestimmt werden.

Um dies zu erreichen, setzen wir in dem Ausdrucke [illegible] für h und i den Werth $\frac{p-1}{3}$ [illegible]

---

*) Setzt man nunmehr [illegible], so nimmt die Gleichung [illegible] die Gestalt

$$4p = A^2 + 27B^2$$

an, und man beweist dann mittelst derselben Betrachtungen, die in der vorigen Vorlesung angewendet worden sind, dass man [illegible] von $4p$ nur auf eine Weise zerlegen [illegible].

$$\psi\left(\frac{p-1}{3}, \frac{p-1}{3}, g\right) \equiv \sum_{\mu=1}^{\mu=p-2} \left(g^{\frac{p-1}{3}}\right)^{\text{ind.}\mu - 2\,\text{ind.}(1+\mu)}$$

$$\equiv \sum_{\mu=1}^{\mu=p-2} \left(g^{\frac{p-1}{3}}\right)^{\text{ind.}(\mu+\mu^2)} \quad (\text{mod. } p).$$

Da aber $g^{k.\frac{p-1}{3}}$ resp. den Zahlen 1, $g^{\frac{p-1}{3}}$, $g^{2.\frac{p-1}{3}}$ (mod. p) congruent ist, jenachdem $k \equiv 0, 1, 2$ (mod. 3) ist, und da die Congruenz stattfindet:

$$(12) \qquad g^{2.\frac{p-1}{3}} + g^{\frac{p-1}{3}} + 1 \equiv 0 \quad (\text{mod. } p),$$

so reducirt sich offenbar jene Summe (mod. p) auf

$$A_0 + A_1 g^{\frac{p-1}{3}} + A_2 g^{2.\frac{p-1}{3}} \equiv a + b \,.\, g^{\frac{p-1}{3}} \quad (\text{mod. } p),$$

wenn A_0, A_1, A_2, a, b dieselben Zahlen sind, wie im Vorhergehenden. Da andererseits wegen der Bedingung $h + k < p - 1$ der Ausdruck $\psi(h, k, g)$ durch p theilbar ist, findet sich

$$(13) \quad A_0 + A_1 g^{\frac{p-1}{3}} + A_2 g^{2.\frac{p-1}{3}} \equiv a + b \,.\, g^{\frac{p-1}{3}} \equiv 0 \quad (\text{mod. } p).$$

Wenn dagegen $h = 2 \,.\, \frac{p-1}{3}$, $k = 2 \,.\, \frac{p-1}{3}$ gesetzt wird, also $h + k > p - 1$ ist, so ergiebt sich

$$\psi\left(2 \,.\, \frac{p-1}{3}, 2 \,.\, \frac{p-1}{3}, g\right) \equiv \sum_{\mu=1}^{\mu=p-2} \left(g^{2.\frac{p-1}{3}}\right)^{\text{ind.}(\mu+\mu^2)} \equiv a + b g^{2.\frac{p-1}{3}}$$
$$(\text{mod. } p),$$

und nach dem Satze in Nr. 2 der vorigen Vorlesung folgende Congruenz:

$$(14) \quad A_0 + A_1 g^{2.\frac{p-1}{3}} + A_2 g^{\frac{p-1}{3}} \equiv a + b g^{2.\frac{p-1}{3}} \equiv -\frac{\prod 2 \,.\, \frac{p-1}{3}}{\left(\prod \frac{p-1}{3}\right)^2}$$
$$(\text{mod. } p).$$

Mit Rücksicht auf die Gleichungen (4) schliesst man aus den Congruenzen (12), (13) und (14) die folgende:

$$(15) \qquad A \equiv -\frac{\prod 2 \,.\, \frac{p-1}{3}}{\left(\prod \frac{p-1}{3}\right)^2} \quad (\text{mod. } p),$$

welche vermittelst der Congruenzen:

$$2.\frac{p-1}{3}+1\equiv-\frac{p-1}{3},\ 2.\frac{p-1}{3}+2\equiv-\left(\frac{p-1}{3}-1\right),\ldots p-1\equiv-1$$
$$(\text{mod. } p)$$

auch so geschrieben werden kann:

$$(16)\qquad A\left(\prod\frac{p-1}{3}\right)^3\equiv-\Pi(p-1)\equiv+1\quad(\text{mod. } p)$$

und dann den später zu benutzenden Satz lehrt, dass die Zahl A cubischer Rest von p ist. In der That, man kann z so wählen, dass $z\,.\prod\left(\frac{p-1}{3}\right)\equiv 1$ (mod. p) wird; durch Multiplication der Congruenz (16) mit z^3 ergiebt sich dann aber $A\equiv z^3$ (mod. p), d. h. A als Rest eines Cubus.

Der Congruenz (13) kann man nachstehende Form geben:

$$A+B\left(1+2g^{\frac{p-1}{3}}\right)\equiv 0\quad(\text{mod. } p)$$

oder auch wegen (12) folgende Form:

$$(17)\qquad A+B\left(g^{\frac{p-1}{3}}-g^{2.\frac{p-1}{3}}\right)\equiv 0\quad(\text{mod. } p),$$

welche je nach der willkürlich getroffenen Wahl der primitiven Wurzel g das Vorzeichen von B bestimmt; denn es ist leicht zu sehen, dass dies Zeichen sich verändert, wenn man statt g eine andere primitive Wurzel γ passend wählt. In der That, alle übrigen primitiven Wurzeln zerfallen in zwei Classen, jenachdem ihr Index von der Form $3n+1$ oder $3n+2$ ist, und dass es in jeder dieser Classen wirklich primitive Wurzeln giebt, folgt daraus, dass $g^{\pm k}$ eine primitive Wurzel ist, wenn k gegen $p-1$ prim ist, und dass dann k durch 3 nicht theilbar ist, also stets eine der beiden Zahlen k und $p-1-k$ die Form $3n+1$, die andere die Form $3n+2$ haben muss. Ersetzt man nun in (17) g durch eine primitive Wurzel γ der zweiten Classe, so ergiebt sich leicht:

$$A-B\left(\gamma^{\frac{p-1}{3}}-\gamma^{2.\frac{p-1}{3}}\right)\equiv 0\quad(\text{mod. } p),$$

wie behauptet wurde.

Durch die Congruenzen (16) und (17) sind nun die Zahlen A, B vollständig bestimmt; denn, da sie der Gleichung $4p=A^2+3B^2$ genügen sollen, so können sie numerisch nicht grösser als $p-1$ sein. Dies erhellt für die beiden ersten Primzahlen von der Form $6n+1$, nämlich $p=7$ und $p=13$, wenn man ihre

Zerlegungen wirklich aufstellt:

$$4 \cdot 7 = 1^2 + 3 \cdot 3^2, \; 4 \cdot 13 = 5^2 + 3 \cdot 3^2;$$

jede grössere Primzahl p von dieser Form aber genügt der Ungleichheit $4 < \frac{p}{4}$; da nun $A^2 < 4p$, $B^2 < \frac{4}{3}p$ ist, wird auch $A^2 < \frac{p^2}{4}$, $B^2 < \frac{1}{3} \cdot \frac{p^2}{4}$ sein müssen, woraus das Behauptete folgt*).
Auf solche Weise gelangt man zu folgendem Satze, welcher dem in Nr. 7 der vorigen Vorlesung ausgesprochenen ganz analog ist:

Bestimmt man A, B als die absolut kleinsten Zahlen, welche den Congruenzen:

$$A.\left(\prod \frac{p-1}{3}\right)^3 \equiv 1, \quad A + B\left(g^{\frac{p-1}{3}} - g^{2 \cdot \frac{p-1}{3}}\right) \equiv 0 \pmod{p}$$

genügen, so zerfällt das Vierfache der Primzahl p von der Form $6n + 1$ nach der Gleichung: $4p = A^2 + 3B^2$ in die Summe eines einfachen und eines dreifachen Quadrates.

Noch muss bemerkt werden, dass sich wieder a priori angeben lässt, mit welchem Vorzeichen die Basis des einfachen Quadrats durch diese Methode erhalten wird; denn, da $A = 2a - b$ ist, folgt aus den Congruenzen $a \equiv -1$, $b \equiv 0 \pmod{3}$ die dritte: $A \equiv +1 \pmod{3}$, welche das fragliche Vorzeichen bestimmt.

Dieser Satz ist bereits in Crelle's J. Bd. 2 in einer kleinen Abhandlung (de residuis cubicis commentatio numerosa) von Jacobi ausgesprochen worden. Er findet sich ferner bewiesen in Cauchy's mém. sur la théorie des nombres, pag. 725, und in Lebesgue's recherches sur les nombres in Liouv. J., Bd. 2, pag. 279. Vgl. auch Stern in Cr. J, Bd. 7, pag. 104, Clausen ebend. Bd. 8, pag. 140, sowie die Bemerkungen von Stern zu dieser letzten Notiz, ebendas. Bd. 9, pag. 97.

4. Endlich wollen wir die Primzahl p von der Form $8n + 1$ voraussetzen. Da sodann $p - 1$ den Theiler 8 hat, dürfen wir diesen für e wählen, und erhalten, wenn wir in der Formel (6) voriger Vorlesung $n = 4$, $h = f = \frac{p-1}{8}$ und $\omega^f = \alpha$ setzen, sodass α eine primitive Wurzel der Gleichung $x^8 = 1$

*) Es folgt auch daraus, dass $A^2 < 4p - 27$ ist, was in der Form $\frac{1}{4}(p^2 - (p-8)^2 - 44)$ geschrieben werden kann. S. Cauchy, mém. s. la th. des nombres.

und $\alpha^4 = -1$ wird, die Gleichung:

$$(18) \qquad p = \sum_{\mu=1}^{\mu=p-2} \alpha^{\text{ind.}\mu + 3\,\text{ind.}(1+\mu)} \cdot \sum_{\mu=1}^{\mu=p-2} \alpha^{-\text{ind.}\mu - 3\,\text{ind.}(1+\mu)},$$

worin die erste Summe den Werth des Ausdrucks

$$(19) \qquad \psi_4(\alpha) = \frac{(\alpha, r) \cdot (\alpha^4, r)}{(\alpha^5, r)}$$

repräsentirt. Multipliciren wir den letztern im Zähler und Nenner mit $(\alpha^3, r) \cdot (\alpha^7, r)$, so kommt:

$$\psi_4(\alpha) = \frac{(\alpha^3, r) \cdot (\alpha^4, r)}{(\alpha^7, r)} \cdot \frac{(\alpha, r) \cdot (\alpha^7, r)}{(\alpha^3, r) \cdot (\alpha^5, r)}.$$

Nun liefert die Formel (29) der 8. Vorlesung, wenn darin successive $h = f$ und $h = 3f$ gesetzt wird, die beiden Gleichungen:

$$(20) \quad (\alpha, r) \cdot (\alpha^7, r) = (-1)^f \cdot p, \quad (\alpha^3, r) \cdot (\alpha^5, r) = (-1)^{3f} \cdot p,$$

aus denen man schliesst, dass die vorige Gleichung einfacher

$$\psi_4(\alpha) = \frac{(\alpha^3, r) \cdot (\alpha^4, r)}{(\alpha^7, r)}$$

d. h.

$$(21) \qquad \psi_4(\alpha) = \psi_4(\alpha^3)$$

ergiebt. Setzt man daher

$$\psi_4(\alpha) = A_0 + A_1\alpha + A_2\alpha^2 + A_3\alpha^3 + A_4\alpha^4 + A_5\alpha^5 + A_6\alpha^6 + A_7\alpha^7$$

oder, mit Rücksicht auf die Gleichung $\alpha^4 = -1$,

$$\psi_4(\alpha) = (A_0 - A_4) + (A_1 - A_5)\alpha + (A_2 - A_6)\alpha^2 + (A_3 - A_7)\alpha^3,$$

so wird

$$\psi_4(\alpha^3) = (A_0 - A_4) + (A_3 - A_7)\alpha - (A_2 - A_6)\alpha^2 + (A_1 - A_5)\alpha^3,$$

und die Vergleichung beider Ausdrücke liefert wegen (21) die Beziehungen:

$$(22) \qquad A_2 - A_6 = 0, \quad A_1 - A_5 = A_3 - A_7.$$

Wenn also zur Abkürzung geschrieben wird:

$$(23) \qquad A_0 - A_4 = a, \quad A_1 - A_5 = A_3 - A_7 = b,$$

so findet man

$$\psi_4(\alpha) = a + b(\alpha + \alpha^3),$$

also auch, da $\alpha^{-1} = \alpha^7 = -\alpha^3$, $\alpha^{-3} = \alpha^5 = -\alpha$ ist,

$$\psi_4(\alpha^{-1}) = a - b(\alpha + \alpha^3)$$

und endlich aus (18) die Gleichung

$$p = a^2 - b^2(\alpha + \alpha^3)^2.$$

Diese vereinfacht sich, wenn man bemerkt, dass

$$(\alpha + \alpha^3)^2 = \alpha^2 + 2\alpha^4 + \alpha^6 = \alpha^2 - 2 - \alpha^2 = -2$$

ist, und nimmt dann die Form an:

$$p = a^2 + 2b^2. \tag{24}$$

Ist also p eine Primzahl von der Form $8n + 1$, so kann sie stets als die Summe aus einem einfachen und einem doppelten Quadrate dargestellt werden.

5. Der Satz in Nr. 2 der vor. Vorl. gestattet nun wieder, die Zahlen a, b, aus deren Quadraten p zusammengesetzt ist, direct zu bestimmen. In der That, setzen wir in der Function $\psi\,(h, k, g)$ zunächst $h = f$, $k = 4f$, so ergiebt sich, da $h + k = 5f$ also $< p - 1$ ist, nach dem ersten der dort unterschiedenen Fälle

$$\psi\,(f, 4f, g) \equiv 0 \pmod{p},$$

während andererseits

$$\psi\,(f, 4f, g) \equiv \sum_{\mu=1}^{\mu=p-2} g^{f(\text{ind.}\mu + 3\,\text{ind.}(1+\mu))} \pmod{p} \tag{25}$$

ist. Geben nun die Zahlen $A_0, A_1, \ldots\ldots A_7$ resp. an, wieoft ind. μ + 3 ind. $(1 + \mu)$ den Zahlen $0, 1, \ldots\ldots 7 \pmod{8}$ congruent wird, so sind sie mit den in der vorigen Nr. ebenso bezeichneten Zahlen identisch, und da ausserdem $g^{4f} = g^{\frac{p-1}{2}} \equiv -1$ (mod. p) ist, wird die Summe auf der rechten Seite der Congruenz mit Rücksicht auf die Gleichungen (22) und (23) leicht dem folgenden Ausdrucke:

$$a + b\,(g^f + g^{3f}) \tag{26}$$

(mod. p) congruent gefunden. Also erhält man

$$a + b\,(g^f + g^{3f}) \equiv 0 \pmod{p}. \tag{27}$$

Wenn zweitens in $\psi\,(h, k, g)$ für h, k die Werthe $7f$, $4f$ gewählt werden, folgt nach dem zweiten Falle desselben Satzes

$$\psi\,(7f, 4f, g) \equiv -\frac{\Pi 5f}{\Pi f\,.\,\Pi 4f} \pmod{p};$$

andererseits ist

$$\psi\,(7f, 4f, g) \equiv \sum_{\mu=1}^{\mu=p-2} g^{f(7\,\text{ind.}\mu + 5\,\text{ind.}(1+\mu))} \equiv \sum_{\mu=1}^{\mu=p-2} g^{7f\,(\text{ind.}\mu + 3\,\text{ind.}(1+\mu))}.$$

Da diese Summe aus der in (25) enthaltenen hervorgeht,

wenn g durch g^7 ersetzt wird, und $g^{7f} = g^{3f} . g^{4f} \equiv - g^{3f}$, $g^{21f} \equiv g^{5f} \equiv - g^f$ ist, findet man nach dem Ausdrucke (26) jener Summe die Beziehung:

$$\psi\,(7f, 4f, g) \equiv a - b\,(g^f + g^{3f}) \pmod{p}$$

und folglich

$$a - b\,(g^f + g^{3f}) \equiv - \frac{\Pi 5f}{\Pi f \,.\, \Pi 4f} \pmod{p}. \tag{28}$$

Aus den Congruenzen (27) und (28) ergiebt sich

$$a \equiv - \tfrac{1}{2} \cdot \frac{\Pi 5f}{\Pi f \,.\, \Pi 4f} \pmod{p}, \tag{29}$$

und sodann liefert die zweite derselben zur Bestimmung von b die Congruenz:

$$b\,(g^f + g^{3f}) \equiv \tfrac{1}{2} \cdot \frac{\Pi 5f}{\Pi f \,.\, \Pi 4f} \pmod{p}\,. \tag{30}$$

Da nun wieder, wie genau durch das in Nr. 7. der vorigen Vorl. angewendete Verfahren erkannt werden kann, a, b die absolut kleinsten Reste sein müssen, welche diesen Congruenzen genügen, sind sie durch dieselben völlig bestimmt, und man findet den Satz:

Man erhält die Zerlegung einer Primzahl p von der Form $8n + 1$ in die Summe eines einfachen und eines doppelten Quadrates nach der Formel (24), wenn man a, b als die absolut kleinsten Werthe bestimmt, welche den Congruenzen

$$a \equiv - \tfrac{1}{2} \cdot \frac{\Pi 5f}{\Pi f \,.\, \Pi 4f},\ b\,(g^f + g^{3f}) \equiv \tfrac{1}{2} \cdot \frac{\Pi 5f}{\Pi f \,.\, \Pi 4f} \pmod{p}$$

Genüge leisten.

6. Endlich lässt sich durch ganz ähnliche Betrachtungen, als wir bei der Zerlegung von p in die Summe zweier Quadrate angewendet haben, nachweisen, dass die so bestimmte Zahl a, welche offenbar ungerade sein muss, durch 4 getheilt, den Rest 3 lässt, wodurch über das Vorzeichen der Basis des einfachen Quadrates, wie sie der vorige Satz liefert, a priori entschieden wird. Geben wir zu diesem Zwecke zunächst dem Ausdrucke (19) die andere Gestalt:

$$\psi_4\,(\alpha) = \frac{(\alpha, r) \,.\, (\alpha^3, r)}{(\alpha^4, r)} \cdot \frac{(\alpha^4, r)^2}{(\alpha^3, r) \,.\, (\alpha^7, r)}$$

und beachten, dass $\alpha^4 = -1$, also $(\alpha^4, r)^2 = (-1, r)^2$ nach

Nr. 3 der 9. Vorlesung gleich p ist, sowie andererseits die Gleichungen (20), so kann man die vorige auch so darstellen:

$$\psi_4(\alpha) = (-1)^f \cdot \psi_3(\alpha), \tag{31}$$

während

$$\psi_3(\alpha) = \sum_{\mu=1}^{\mu=p-2} \alpha^{\text{ind.}\mu + 4\,\text{ind.}(1+\mu)}$$

ist. Schreiben wir einfacher

$$\psi_3(\alpha) = \sum \alpha^{\lambda+4k},$$

wo $\lambda = \text{ind.}\,\mu$, $k = \text{ind.}\,(1+\mu)$ gesetzt ist, so hat λ alle Werthe $0, 1, 2, \ldots . p-2$ zu durchlaufen, mit einziger Ausnahme von $\frac{p-1}{2}$, und k ist jedesmal durch die Congruenz

$$g^k \equiv 1 + g^\lambda \pmod{p}$$

zu bestimmen. Denkt man sich ferner $\psi_3(\alpha)$ auf die Form

$$A + B(\alpha + \alpha^3)$$

gebracht, welche es nach der Gleichung

$$\psi_4(\alpha) = a + b(\alpha + \alpha^3)$$

haben muss, da es sich von $\psi_4(\alpha)$ höchstens durch das Vorzeichen unterscheidet, so ist zuerst:

$$a = (-1)^f \cdot A; \tag{32}$$

A aber erhält man offenbar, wenn man in der Summe, welcher $\psi_3(\alpha)$ gleich ist, λ nur alle zulässigen Vielfachen von 4 oder, wenn $\lambda = 4\lambda'$ gesetzt wird, λ' die Werthe $0, 1, 2, \ldots . 2f-1$ mit Ausnahme von f durchlaufen lässt, wodurch man, da $\alpha^{4m} = +1$ oder $= -1$ ist, jenachdem m gerade oder ungerade ist,

$$A = \sum (-1)^{\lambda'+k} \tag{33}$$

findet. Dabei muss λ' die angezeigten Werthe durchlaufen und k jedesmal durch die Congruenz:

$$g^k \equiv 1 + g^{4\lambda'} \pmod{p}$$

bestimmt werden. Ist nun zuerst $\lambda' = 0$, so wird $g^k \equiv 2 \pmod{p}$, und da (nach Nr. 3, 15. V.) 2 quadratischer Rest von p ist, wird k gerade, das entsprechende Glied der Summe also gleich $+1$ sein. Die übrigen Werthe von λ' können paarweise so zusammen-

gefasst werden, dass $f - \nu$, $f + \nu$ ein Paar bilden und man alle Werthe von λ' erhält, wenn ν die Reihe 1, 2, 3 .... $f - 1$ durchläuft. Seien k^0, k' die zu einem Paare gehörigen Werthe des k; dann findet man:

$$g^{k^0+k'} \equiv (1 + g^{4(f-\nu)}) (1 + g^{4(f+\nu)}) \equiv g^{4(f-\nu)} . (1 + g^{4(f+\nu)})^2 \pmod{p}$$

d. h. $g^{k^0+k'}$ ist quadratischer Rest (mod. p), $k^0 + k'$ gerade und k^0, k' gleichzeitig gerade oder gleichzeitig ungerade. Daher lässt sich, wie leicht zu sehen, die Gleichung (33) auch folgendermassen schreiben:

$$A = 1 + \sum_{\nu=1}^{\nu=f-1} [(-1)^{f-\nu+k^0} + (-1)^{f+\nu+k'}] = 1 + 2 . \sum_{\nu=1}^{\nu=f-1} (-1)^{\nu+k'} . (-1)^f.$$

Wenn demnach N bezeichnet, wieoft der Exponent $\nu + k'$ ungerade ausfällt, folgt hieraus

$$A = 1 + (-1)^f . (2f - 2 - 4N),$$

also nach (32):

$$a \equiv (-1)^f + 2(f - 1) \pmod{4},$$

welche Congruenz in beiden möglichen Fällen, ob f gerade oder ungerade sei, wie behauptet worden ist,

$$a \equiv -1 \pmod{4}$$

ergiebt.

Zum Schluss mag erwähnt werden, dass die Anzahl a auch noch durch eine, etwas von der Congruenz (29) verschiedene Congruenz definirt werden kann. Zu der Function $\psi_3(\alpha)$ stehen nämlich die Ausdrücke

$$\psi(f, 3f, g), \quad \psi(7f, 5f, g)$$

in derselben Beziehung wie die Ausdrücke

$$\psi(f, 4f, g), \quad \psi(7f, 4f, g)$$

zur Function $\psi_4(\alpha)$. Verfährt man nun genau ebenso wie in Nr. 5, so erhält man die Congruenzen:

$$\left.\begin{aligned} A + B(g^f + g^{3f}) &\equiv 0 \\ A - B(g^f + g^{3f}) &\equiv -\frac{\Pi 4f}{\Pi f \, \Pi 3f} \end{aligned}\right\} \pmod{p},$$

woraus nach der Gleichung (32)

$$(34) \qquad 2a \equiv (-1)^{f+1} . \frac{\Pi 4f}{\Pi f . \Pi 3f} \pmod{p}$$

hervorgeht.

Die, in den letzten drei Nummern abgeleiteten Resultate finden sich in Jacobi's Abhandlung im Cr. J. Bd. 30*), nur die zweite Congruenz, welche zur Bestimmung von a gefunden worden ist, nebst noch einer andern ist von Stern**) angegeben worden.

Zwölfte Vorlesung.

Die complexen ganzen Zahlen von der Form $a + bi$.

1. Wir kehren nunmehr wieder zur Theorie der Potenzreste zurück und beginnen unsere weitern Untersuchungen mit der Betrachtung der biquadratischen Reste.

Eine gegen p prime Zahl m heisst biquadratischer Rest oder Nichtrest (mod. p), jenachdem die Congruenz $x^4 \equiv m$ (mod. p) möglich ist oder nicht. Die Entscheidung dieser Frage kommt hauptsächlich wieder, wie bei den quadratischen Resten, auf die speciellere zurück, ob eine gegebene Primzahl von einer andern Primzahl biquadratischer Rest sei, oder Nichtrest. Als Gauss, welcher zuerst Untersuchungen darüber angestellt hat,***) diese Fragen in Angriff nahm, boten sich ihm zwar für eine Menge specieller Fälle einzelne Sätze dar, jedoch konnte er durchaus kein gemeinsames Band zwischen ihnen entdecken, wodurch er dahin hätte geführt werden können, das hier herrschende allgemeine Gesetz aufzustellen. Endlich — man vermuthet, dass gleichzeitige Untersuchungen über die Theorie der elliptischen Functionen ihm den Gedanken geboten haben — fand er das richtige Princip und that einen Schritt, den man stets der höchsten Bewunderung werth halten wird, und welcher

---

*) Vgl. auch in the Report of the British Association for the advancement of science, Jahrg. 1863, den Report on the theory of numbers von Smith, Nr. 121. Cauchy, mém. sur la theorie des nombres, note 13.

**) in Crelle's J. Bd. 32 pag. 89.

***) In seiner ersten Abhandlung theoria residuorum biquadraticorum, math. Werke, Bd. 2.

gewissermassen der Zahlentheorie eine ganz neue Welt eröffnet hat: er verliess den Boden der reellen Zahlen und führte die sogenannten (einfachsten) complexen Zahlen ein, nämlich die Zahlen von der Form $a + bi$, in welcher a, b reelle ganze Zahlen, i aber das Zeichen $\sqrt{-1}$ bedeutet. Sobald man diese Zahlen, welche bei den gedachten Untersuchungen die Rolle der Elemente spielen, in die Betrachtung einführt, nimmt Alles einen ganz einfachen Character an und gehorcht ganz ähnlichen Gesetzen, als wir sie bei den quadratischen Resten gefunden haben. Hierin allein schon liegt die Berechtigung, ja die Nothwendigkeit für die Einführung der complexen Zahlen, auch wenn nicht andere Umstände, auf welche einzugehen hier nicht der Ort ist, sie bestätigten. Bemerken wir in dieser Beziehung nur, dass schon die Untersuchungen, welche wir in der 10. Vorlesung angestellt haben, von einer andern Seite her die Erkenntniss geliefert haben, wie die complexen Zahlen sich naturgemäss der Betrachtung darbieten, ja aufdrängen. Indem wir sie daher hier den Untersuchungen über biquadratische Reste zu Grunde legen, müssen wir vor Allem die Principien ihrer Theorie entwickeln. Dabei dürfen wir die Regeln, nach welchen die einfachsten Rechnungsoperationen mit complexen Grössen zu vollziehen sind, als bekannt voraussetzen und uns hinsichtlich ihrer Theorie auf diejenigen Sätze und Bemerkungen beschränken, welche für das Folgende wesentlich sind. Ausführlicheres darüber findet man in Gauss' 2[ter] Abhandlung über biquadratische Reste*) oder in Dirichlet's Abhandlung: recherches sur les formes quadratiques à coëfficiens et à indéterminées complexes in Cr. J. Bd. 24, besonders aber in einem Schulprogramm des collége royal francais zu Berlin**), welches eine Dirichlet'sche Vorlesung über die Theorie der complexen Zahlen reproducirt.

2. 1) Zwei complexe Zahlen $a + bi$ und $a - bi$, welche sich nur durch das Vorzeichen von i von einander unterscheiden, heissen conjugirte complexe Zahlen und das Product derselben:

*) Theoria residuorum biquadraticorum commentatio II in Gauss' W. Bd. II.

**) Vom Jahre 1863: élémens de la théorie des nombres complexes de la forme $a + b\sqrt{-1}$, d'après un cours de M. Dirichlet, par G. Arendt.

$$(a + bi)(a - bi) = a^2 + b^2$$

heisst ihre Norm. Diese soll durch $N(a + bi)$ bezeichnet werden; offenbar ist $N(a + bi) = N(a - bi)$.

2) Jede complexe Zahl, deren Norm der Einheit gleich ist, soll eine complexe Einheit heissen; aus der Gleichung $a^2 + b^2 = 1$ findet sich leicht, dass es nur vier complexe Einheiten giebt, nämlich $+1, -1, +i, -i$.

3) Die Zwei ist in der Theorie der complexen Zahlen nach der identischen Gleichung:

$$2 = (1 + i)(1 - i) = -i(1 + i)^2$$

noch in Factoren zerlegbar.

4) Eine complexe Zahl $a + bi$, bei welcher a und b gerade sind, soll gerade genannt werden. Jede gerade complexe Zahl ist also durch Zwei theilbar, und offenbar auch umgekehrt. Eine Zahl $a + bi$ aber, bei welcher a und b ungerade sind, soll halbgerade heissen; jede halbgerade complexe Zahl ist durch $1 + i$ theilbar; denn, setzt man $a = 2\alpha + 1$, $b = 2\beta + 1$, so findet man

$$a + bi = 1 + i + 2(\alpha + \beta i) = (1 + i)(1 + \alpha + \beta + i(\beta - \alpha)).$$

Umgekehrt ist jede durch $1 + i$ theilbare complexe Zahl entweder eine gerade, oder eine halb-gerade complexe Zahl; denn, setzt man

$$a + bi = (1 + i)(A + Bi),$$

so folgt $a = A - B$, $b = A + B$, diese beiden Zahlen sind aber entweder gleichzeitig gerade oder gleichzeitig ungerade, da ihre Summe durch 2 aufgeht. Eine complexe Zahl $a + bi$ endlich, in der von den Zahlen a, b die eine gerade, die andere ungerade ist, soll ungerade genannt werden.

5) Multiplicirt man mit den vier Einheiten die complexe Zahl $a + bi$, so entsteht eine Gruppe von vier Zahlen:

$$a + bi,\ -a - bi,\ -b + ai,\ b - ai,$$

welche associirt genannt werden sollen.

6) Eine complexe Zahl $a + bi$ soll primär heissen, wenn $a - 1$ und b durch 4 getheilt entweder gleichzeitig den Rest Null oder gleichzeitig den Rest Zwei lassen. Conjugirte Zahlen sind immer gleichzeitig primär oder nicht primär.

7) In jeder Gruppe associirter ungerader Zahlen

$$a + bi, \; -a - bi, \; -b + ai, \; b - ai$$

giebt es eine primäre Zahl. Ist nämlich etwa a gerade, b ungerade, so ist eine der Zahlen $+b$, $-b$ von der Form $4n + 1$, die andere von der Form $4n + 3$; ist also a durch 2, aber nicht durch 4 theilbar, so wird diejenige der beiden Zahlen $b - ai$, $-b + ai$ primär sein, in welcher der reelle Theil die Form $4n + 3$ hat; wenn dagegen a durch 4 theilbar ist, so wird die andere jener Zahlen primär, bei welcher der reelle Theil von der Form $4n + 1$ ist. Und ähnlich verhält sich's in jedem andern Falle. Ist $b = 0$, die complexe Zahl also reell, so reducirt sich die Gruppe der associirten Zahlen auf zwei: $+a$ und $-a$, von welchen diejenige primär ist, welche die Form $4n + 1$ hat.

8) **Eine Zahl soll als complexe Primzahl bezeichnet werden, wenn es nicht möglich ist, sie in zwei, reelle oder complexe, Factoren zu zerlegen, welche Beide von complexen Einheiten verschieden sind.**

3. Der Grund, warum bei Einführung der complexen Zahlen die Lehre von den biquadratischen Resten sich einfacher gestaltet, liegt darin, dass hier die reellen Primzahlen noch nicht die einfachsten Elemente der Untersuchung sind, sich vielmehr, als complexe Zahlen aufgefasst, noch weiter zerlegen lassen, wie dies soeben für die Zwei schon gezeigt wurde. Die Primzahlen q von der Form $4n + 3$ behalten freilich auch hier die Bedeutung von Primfactoren. Denn, setzen wir

$$q = (a + bi)(\alpha + \beta i), \tag{1}$$

so ist zunächst zu bemerken, dass in keinem der Factoren die reellen Elemente gleichzeitig durch q theilbar sein können; denn, wäre z. B. $a = a'q$, $b = b'q$, so würde

$$q = q(a' + b'i)(\alpha + \beta i),$$

woraus auch

$$q = q(a' - b'i)(\alpha - \beta i),$$

also

$$q^2 = q^2(a'^2 + b'^2)(\alpha^2 + \beta^2)$$

d. h. $a'^2 + b'^2 = 1$, $\alpha^2 + \beta^2 = 1$ oder $a' + b'i$, $\alpha + \beta i$ gleich Einheiten werden würden; die Zerlegung von q in complexe Factoren wäre also keine eigentliche Zerlegung. Dies vorausgeschickt, findet sich aus (1)

$$q^2 = (a^2 + b^2)(\alpha^2 + \beta^2),$$

also etwa $a^2 + b^2 \equiv 0$ (mod. q). Da hier weder a noch b durch q theilbar sein darf, so bestimme man B, was möglich ist, durch die Congruenz $b\,B \equiv 1$ (mod. q), dann findet man $(a\,B)^2 \equiv -1$ (mod. q) d. h. -1 wäre quadratischer Rest von q, gegen den in Nr. 2 der 9. Vorlesung erhaltenen Satz.

Dagegen wissen wir aus der Formel (15) der 10. Vorlesung, dass jede reelle Primzahl p von der Form $4n + 1$ in der Form $a^2 + b^2$ darstellbar, also in das Product zweier conjugirt-complexer Factoren $a + bi$, $a - bi$ zerlegbar ist. Diese spielen nun aber wieder die Rolle von Primfactoren; denn könnte man weiter zerlegen und setzen:

$$a + bi = (\alpha + \beta i)\,(\alpha' + \beta' i),$$

ohne dass einer der Factoren eine Einheit ist, so fände man

$$p = (\alpha^2 + \beta^2)\,.\,(\alpha'^2 + \beta'^2),$$

also eine Zerlegung der Primzahl p in zwei, von Eins verschiedene, reelle Factoren, was nicht angeht.

In der Theorie der complexen Zahlen von der Form $a + bi$ finden wir also neben der Primzahl $1 + i$ zwei Arten von Primfactoren: die reellen Primzahlen von der Form $4n + 3$ und die complexen Factoren der Primzahlen von der Form $4n + 1$. Da letztere offenbar ungerade complexe Zahlen sind, werden sie, mit einer passenden Einheit multiplicirt, primär. Die reellen Primzahlen von der Form $4n + 3$ werden primär, wenn sie negativ genommen werden. Jede complexe Zahl kann nur auf eine einzige Weise als Product solcher (primärer) Primzahlen dargestellt werden. Dieser Hauptsatz gründet sich auf die folgende Betrachtung:

4. Sind $m = a + bi$ und $m_1 = a_1 + b_1 i$ zwei beliebige complexe Zahlen, so giebt es stets eine complexe Zahl $z = x + yi$ von der Art, dass

$$N\,(m - m_1 z) \overline{\gtrless} \tfrac{1}{2}\,N\,(m_1)$$

ist. Denn, ist x die ganze Zahl, welche dem reellen Theile, y diejenige, welche dem Coëfficienten von i in dem Quotienten

$$\frac{a + bi}{a_1 + b_1 i} = \frac{a a_1 + b b_1}{a_1^2 + b_1^2} + i\,.\,\frac{a_1 b - a b_1}{a_1^2 + b_1^2}$$

am Nächsten liegt, und setzt man $\frac{m}{m_1} - z = \alpha + \beta i$, so werden α, β numerisch nicht grösser als $\frac{1}{2}$, also auch $N\left(\frac{m}{m_1} - z\right) = \alpha^2 + \beta^2$

nicht grösser als $\frac{1}{2}$ sein, und folglich, wie behauptet wurde, $N(m - m_1 z) \overline{\gtrless} \frac{1}{2} N(m_1)$.

Setzt man nun die ganze complexe Zahl $m - m_1 z = m_2$, so ist $N(m_2) \overline{\gtrless} \frac{1}{2} N(m_1)$. Dieser Satz gestattet, eine Reihe von Gleichungen aufzustellen:

$$m = m_1 z + m_2$$
$$m_1 = m_2 z_1 + m_3$$
$$m_2 = m_3 z_2 + m_4$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad ,$$

welche lauter ganze complexe Zahlen enthält, von denen die Zahlen $m_1, m_2, m_3, m_4, \ldots$ den Bedingungen

$$N(m_2) \overline{\gtrless} \tfrac{1}{2} N(m_1),\ N(m_3) \overline{\gtrless} \tfrac{1}{2} N(m_2), \ldots$$

Genüge leisten, und welche eben deswegen nach einer endlichen Anzahl von Gliedern abbrechen muss. Diese Gleichungen dienen, gerade wie in der reellen Zahlentheorie, zur Berechnung des grössten gemeinsamen Theilers der beiden complexen Zahlen m und m_1, und bilden die Grundlage für alle Sätze über Theilbarkeit der complexen Zahlen durch andere, sowie für ihre Zerlegbarkeit in Primfactoren und dergl.

Bemerken wir hier allgemein, dass, wenn in der Theorie irgend welcher complexer Zahlen, deren es unendlich viel verschiedene Arten giebt, wie wir denn noch in diesen Vorlesungen einige andere werden kennen lernen, ein ähnlicher endlicher Algorithmus zur Bestimmung des grössten gemeinsamen Theilers zweier Zahlen besteht, ganz dieselben Sätze über Theilbarkeit und Zerlegbarkeit in Primfactoren daraus gefolgert werden können, als in der reellen Zahlentheorie. Man vergl. darüber Dirichlet's Vorlesungen über Zahlentheorie herausg. von Dedekind, Abschnitt I. Namentlich gilt dann stets, also auch für die complexen Zahlen $a + bi$, der Hauptsatz, dass eine complexe Zahl nur auf eine Weise in die complexen Primfactoren zerlegbar ist; da jedoch jeder Primfactor mit einer beliebigen Einheit multiplicirt gedacht werden kann, so muss der Satz, damit er genau sei, auf primäre Primfactoren bezogen werden, indem man aus allen associirten d. h. nur durch Einheiten verschiedenen Primfactoren einen bestimmten als primär bezeichnet.

Nun ist eine Zahl $m = a + bi$, in welcher sowohl a als b von Null verschieden, solange zerlegbar, als $N(a + bi)$ noch in reelle Factoren zerlegbar ist. In der That, ist

$$(a + bi)(a - bi) = r \cdot s,$$

so kann $a + bi$ keine Primzahl sein, denn sonst müsste, von Einheiten abgesehen, nach dem eben genannten Hauptsatze etwa $a + bi$ gleich r, d. h. $m = r \cdot i^{\varrho}$ sein, wo ϱ einen der Werthe 0, 1, 2, 3 annehmen kann, woraus entweder a oder b gegen die Voraussetzung sich gleich Null ergäbe.

Hiernach kann eine complexe Zahl nur dann eine Primzahl sein, wenn entweder ihre Norm eine reelle Primzahl, oder sie selbst, von Einheiten abgesehen, einer reellen Primzahl gleich ist. Verbindet man dies Resultat mit den Ergebnissen der vorigen Nummer, so folgt leicht, dass ausser den dort angegebenen complexen Primzahlen keine andern existiren, und daraus der am Ende der Nummer ausgesprochene Satz.

Zusatz: Eine Primzahl p von der Form $4n+1$ kann also auch nur auf eine Weise in primäre Primfactoren zerlegt, nämlich nach der 10. Vorlesung als Product zweier primärer conjugirt-complexer Factoren dargestellt werden. Sind diese $a+bi$ und $a-bi$, so ist $p = a^2 + b^2$. Dies lässt sich daher, in Uebereinstimmung mit Nr. 4 der 10. Vorlesung auch so aussprechen: Eine Primzahl p von der Form $4n + 1$ kann nur auf eine Weise in die Summe zweier Quadratzahlen zerlegt werden.

5. Nennen wir zwei complexe Zahlen n und n' in Bezug auf eine dritte complexe Zahl $m = a + bi$ als Modulus congruent oder incongruent, jenachdem die Differenz $n - n'$ durch m theilbar ist oder nicht, so gelten die Regeln für die einfachsten Rechnungen mit Congruenzen als Folgerungen der vorigen Sätze gerade, wie in der reellen Zahlentheorie. Man beweist z. B. auch auf demselben Wege, wie in Nr. 7 der 4. Vorlesung für reelle Zahlen geschehen ist, dass eine Congruenz

$$x^n + a_1 x^{n-1} + \dots + a_n \equiv 0 \pmod{m},$$

in welcher m eine complexe Primzahl, die Coëfficienten complexe Zahlen sind, nicht mehr als n incongruente Wurzeln haben kann.

Alle Zahlen $x + yi$, welche der gegebenen Zahl $\alpha + \beta i$

mod. $(a + bi)$ congruent sind, werden nach der Definition durch folgende Gleichung erhalten:

$$x + yi = (a + bi)(t + ui) + \alpha + \beta i,$$

wenn in derselben t, u alle ganzzahligen Werthe annehmen. Da sich

$$x = at - bu + \alpha, \quad y = au + bt + \beta$$

ergiebt, so wird $y \equiv \beta$ (mod. d) sein, wenn d den grössten gemeinsamen Theiler von a, b bedeutet. Sei y_0 diejenige Lösung dieser Congruenz, welche kleiner als d ist, also y_0 aus der Reihe:

(y) $$0, 1, 2, 3 \ldots . d - 1;$$

dann giebt es ganze Zahlen t, u, welche der Gleichung $au + bt = y_0 - \beta$ genügen und, wenn t_0, u_0 eine bestimmte Lösung derselben ist, sind

$$t = t_0 + \frac{a}{d}z, \quad u = u_0 - \frac{b}{d}z$$

für ein beliebiges ganzzahliges z alle ihre Lösungen. Setzt man nun

$$x_0 = at - bu + \alpha = at_0 - bu_0 + \alpha + \frac{N(m)}{d} \cdot z,$$

so lässt sich z ganz bestimmt so wählen, dass x_0 eine Zahl aus der Reihe:

(x) $$0, 1, 2, 3, \ldots . \frac{N(m)}{d} - 1$$

wird. Da $x_0 + y_0 i$ aber $\alpha + \beta i$ mod. $(a + bi)$ congruent ist, so ergiebt sich das Resultat: dass jede ganze Zahl $\alpha + \beta i$ mod. $(a + bi)$ einer einzigen Zahl $x + yi$ congruent ist, in welcher x, y resp. den Reihen (x), (y) angehören.

Alle $N(m)$ Zahlen $x + yi$, welche entstehen, indem man die $\frac{N(m)}{d}$ Werthe des x mit allen d Werthen des y combinirt, sind also unter einander incongruent, haben aber die Eigenschaft, dass jede andere Zahl einer von ihnen mod. $(a + bi)$ congruent ist. Theilt man daher alle Zahlen in Rest-Classen, indem man die unter einander mod. $(a + bi)$ congruenten in eine Classe zusammenfasst, so ist die Anzahl aller Rest-Classen gleich $N(a + bi)$. Ein System von $N(a + bi)$ unter einander incongruenten, also den einzelnen verschiedenen Classen angehörigen Zahlen soll ein Restsystem mod. $(a + bi)$ genannt werden. Die Zahlen $x + yi$ bilden ein solches.

Es verdient noch bemerkt zu werden, dass für eine zwei-

gliedrige complexe Primzahl $a + bi$ die incongruenten Zahlen $x + yi$ mit den Zahlen

$$0, 1, 2, 3, \ldots . N(a + bi) - 1$$

zusammenfallen, da a und b keinen andern gemeinsamen Theiler, als $d = 1$ haben können, also y gleich Null, x aus der vorigen Reihe zu wählen ist.

6. Jetzt bedeute m eine ungerade complexe Primzahl und μ ihre Norm. In einem Restsysteme (mod. m) bleiben nach Ausschluss des einzigen, durch m theilbaren Gliedes $\mu - 1$ Glieder, welche $r_1, r_2 \ldots . r_{\mu-1}$ heissen mögen und relative Primzahlen zu m sind. Dasselbe gilt daher auch von ihrem Producte $r_1 r_2 \ldots . r_{\mu-1}$. Ist nun n irgend eine durch m nicht theilbare Zahl, so werden, wie leicht zu sehen, die Producte $nr_1, nr_2, \ldots . nr_{\mu-1}$ sämmtlich incongruent und folglich, von der Reihenfolge abgesehen, mit den Resten $r_1, r_2, \ldots . r_{\mu-1}$ congruent sein. Daraus folgt offenbar die Congruenz:

$$n^{\mu-1} . r_1 r_2 \ldots . r_{\mu-1} \equiv r_1 r_2 \ldots . r_{\mu-1} \text{ (mod. } m)$$

oder einfacher:

(2) $$n^{\mu-1} \equiv 1 \text{ (mod. } m),$$

welche Congruenz das Analogon des Fermat'schen Satzes in der Theorie der complexen Zahlen ausspricht. Unterscheiden wir die beiden Hauptfälle, welche die complexen Primzahlen darbieten, so ist

für eine zweigliedrige Primzahl $a + bi$, deren Norm eine reelle Primzahl p von der Form $4n + 1$ ist,

(2a) $$n^{p-1} \equiv 1 \text{ mod. } (a + bi);$$

für eine reelle Primzahl q von der Form $4n + 3$:

(2b) $$n^{q^2-1} \equiv 1 \text{ (mod. } q).$$

Zum Beweise dieser Sätze kann man sich auch einfach des binomischen Lehrsatzes bedienen; denn, nach Weglassung aller durch p theilbaren Glieder, besteht die Congruenz:

$$(\alpha + \beta i)^p \equiv \alpha^p + \beta^p . i^p \text{ (mod. } p),$$

also, weil $i^p = i$ und nach dem Fermat'schen Lehrsatze $\alpha^p \equiv \alpha$, $\beta^p \equiv \beta$ (mod. p) ist, auch die folgende:

$$(\alpha + \beta i)^p \equiv \alpha + \beta i \text{ (mod. } p),$$

aus welcher, da $a + bi$ ein Factor des Modulus p ist, umsomehr

die Congruenz

$$(\alpha+\beta i)^p \equiv \alpha+\beta i \pmod{a+bi}$$

und, wenn $\alpha+\beta i$ relative Primzahl zu $a+bi$ ist, die zu beweisende Congruenz

$$(\alpha+\beta i)^{p-1} \equiv 1 \text{ mod. } (a+bi)$$

hervorgeht.

Dagegen schliesst man für eine Primzahl q von der Form $4n+3$ die folgende Congruenz:

$$(\alpha+\beta i)^q \equiv \alpha-\beta i \pmod{q}$$

und, indem man diese nochmals zur q^{ten} Potenz erhebt,

$$(\alpha+\beta i)^{q^2} \equiv (\alpha-\beta i)^q \equiv \alpha+\beta i \pmod{q},$$

folglich, wenn $\alpha+\beta i$ durch q nicht theilbar ist, die andere zu beweisende Congruenz:

$$(\alpha+\beta i)^{q^2-1} \equiv 1 \pmod{q}.$$

7. Da μ oder $N(m)$ entweder gleich p oder gleich q^2 ist, hat es stets die Form $4n+1$, also ist $\frac{\mu-1}{4}$ eine ganze Zahl. Daher lässt sich die Congruenz (2) auch folgendermassen schreiben:

$$\left(n^{\frac{\mu-1}{4}}-1\right)\cdot\left(n^{\frac{\mu-1}{4}}-i\right)\cdot\left(n^{\frac{\mu-1}{4}}+1\right)\cdot\left(n^{\frac{\mu-1}{4}}+i\right)\equiv 0 \pmod{m}.$$

Da jene Congruenz nun genau $\mu-1$ Wurzeln hat, welche sich auf die vier Factoren vertheilen, und nach Nr. 5 eine Congruenz in Beziehung auf einen Primzahlmodulus nicht mehr Wurzeln haben kann, als ihr Grad beträgt, so hat jede der vier Congruenzen:

$$(3)\quad n^{\frac{\mu-1}{4}} \equiv 1,\ n^{\frac{\mu-1}{4}} \equiv i,\ n^{\frac{\mu-1}{4}} \equiv -1,\ n^{\frac{\mu-1}{4}} \equiv -i \pmod{m},$$

welche für $\varrho = 0, 1, 2, 3$ in der gemeinsamen Form:

$$(4)\qquad n^{\frac{\mu-1}{4}} \equiv i^\varrho \pmod{m}$$

enthalten sind, genau $\frac{\mu-1}{4}$ Wurzeln. Alle Reste (mod. m) zerfallen also in vier Classen von gleichviel Gliedern, welche je der ersten, zweiten, dritten und vierten jener Congruenzen Genüge leisten.

Die Zahlen der ersten Classe sind die biquadratischen Reste (mod. m). Um diesen Satz zu beweisen, bemer-

ken wir erstens, dass, wenn $n \equiv z^4$ (mod. m) ist, daraus $n^{\frac{\mu-1}{4}} \equiv z^{\mu-1} \equiv 1$ (mod. m) sich ergiebt; also gehört jeder biquadratische Rest zur ersten Classe. — Um aber auch zweitens umgekehrt nachzuweisen, dass jede Zahl der ersten Classe biquadratischer Rest sei, braucht nur gezeigt zu werden, dass genau $\frac{\mu-1}{4}$ solcher Reste existiren. Dazu dient die Bemerkung, dass man ein System von $\mu-1$ incongruenten Resten, welche durch m nicht theilbar sind, aus vier Gruppen von $\frac{\mu-1}{4}$ Zahlen zusammensetzen kann, dergestalt, dass, wenn r die Zahlen der ersten Gruppe sind, ir die der zweiten, $-r$ die der dritten, $-ir$ die der vierten Gruppe sein werden. Denn, wählt man irgend eine durch m nicht theilbare Zahl r, so werden die vier Zahlen r, ir, $-r$, $-ir$ (mod. m) incongruent sein, wie man sehr leicht daraus schliesst, dass m eine ungerade Zahl ist. Nimmt man nun eine Zahl r', welche weder durch m theilbar, noch einer dieser vier Zahlen (mod. m) congruent ist, so werden die vier Zahlen r', ir', $-r'$, $-ir'$ sowohl unter einander als auch mit der vorigen Gruppe von Zahlen incongruent sein; denn wäre z. B. $ir' \equiv -ir$, so folgte $r' \equiv -r$ gegen die Voraussetzung. Dieses Verfahren kann, da die Anzahl aller nicht durch m theilbaren Reste gleich $\mu-1$ ist, soweit fortgesetzt werden, bis $\frac{\mu-1}{4}$ Gruppen von vier Zahlen gebildet sind, und giebt dann den Beweis des Behaupteten.

Denkt man sich darauf alle Zahlen des eben angegebenen Restsystems zur vierten Potenz erhoben, so werden die Reste der Biquadrate (mod. m) alle möglichen incongruenten biquadratischen Reste repräsentiren, jeden derselben aber genau viermal liefern, da einerseits je vier Zahlen r, ir, $-r$, $-ir$ dieselbe 4te Potenz haben, andrerseits aus der Congruenz $r'^4 \equiv r^4$ (mod. m), welche auch in der Form

$$(r'-r)(r'-ir)(r'+r)(r'+ir) \equiv 0 \quad (\text{mod. } m)$$

geschrieben werden kann, sich r' einer der Zahlen r, ir, $-r$, $-ir$ congruent, d. h. das Resultat ergiebt, dass nur die vier Zahlen r, ir, $-r$, $-ir$ denselben biquadratischen Rest geben können. Hieraus folgt, dass genau $\frac{\mu-1}{4}$ biquadratische Reste existiren.

Die Zahlen der ersten und dritten Classe zusammengenommen sind die Wurzeln der Congruenz

(5) $$n^{\frac{\mu-1}{2}} \equiv 1 \pmod{m},$$

welche aus der ersten und dritten der Congruenzen (3) durch Quadrirung hervorgeht, und bilden die quadratischen Reste. Ebenso genügen die Zahlen der zweiten und vierten Classe der Congruenz

(6) $$n^{\frac{\mu-1}{2}} \equiv -1 \pmod{m}$$

und sind die quadratischen Nichtreste. Denn, aus der Zusammensetzung des vorher benutzten Restsystems geht hervor, dass je zwei Zahlen r und $-r$ und nur diese denselben quadratischen Rest geben, die Anzahl der quadratischen Reste also gleich $\frac{\mu-1}{2}$ ist. Jede Zahl n aber, welche einem Quadrate $z^2 \pmod{m}$ congruent ist, liefert $n^{\frac{\mu-1}{2}} \equiv z^{\mu-1} \equiv 1 \pmod{m}$ und genügt also der Congruenz (5), die quadratischen Nichtreste demnach der Congruenz (6).

8. Die Potenz i^ϱ, welche in der Congruenz (4) zu wählen ist, soll im Folgenden der biquadratische Character von n heissen und durch das Zeichen*) $\left(\left(\frac{n}{m}\right)\right)$ bezeichnet werden, sodass stets:

(7) $$n^{\frac{\mu-1}{4}} \equiv \left(\left(\frac{n}{m}\right)\right) \pmod{m}$$

ist. Der quadratische Character, welcher $+1$ oder -1 ist, jenachdem n der Congruenz (5) oder (6) genügt, mag auch hier durch das Legendre'sche Zeichen $\left(\frac{n}{m}\right)$ ausgedrückt werden, da eine Verwechslung mit der gleichen, auf die reelle Zahlentheorie bezüglichen Bezeichnung im Folgenden nicht zu befürchten ist. Da nun ein quadratischer Rest zur ersten oder dritten Classe gehört, also den biquadratischen Character ± 1 hat, jeder quadratische Nichtrest aber, als zur zweiten oder vierten Classe

*) Diese Bezeichnung ist den Jacobi'schen Vorlesungen über Zahlentheorie entnommen.

gehörig, einen der biquadratischen Charactere $+i$ oder $-i$ besitzt, so ist offenbar:

$$(8) \qquad \left(\frac{n}{m}\right) = \left(\left(\frac{n}{m}\right)\right)^2.$$

Der biquadratische Character einer Zahl n kann auf analoge Weise ausgedrückt werden, als das Gauss'sche Lemma (s. 9. Vorlesung Nr. 9) den quadratischen Character bestimmt. Denkt man sich wieder das Restsystem der vorigen Nr. und eine durch m nicht theilbare Zahl n, so werden die $\frac{\mu-1}{4}$ Zahlen $n \,.\, r$ zum Theil Zahlen der Gruppe r, zum andern Theil Zahlen der Gruppe ir, dann wieder Zahlen der Gruppe $-r$, und zum letzten Theile Zahlen der Gruppe $-ir$ congruent sein. Das geschehe resp. $\alpha, \beta, \gamma, \delta$ Mal. Es wird behauptet, dass

$$(9) \qquad \left(\left(\frac{n}{m}\right)\right) = i^{\beta+2\gamma+3\delta}$$

sei.

In der That, bezeichnet allgemein ϱ die α Zahlen der Gruppe r, $i\varrho'$ die β Zahlen der Gruppe ir, $-\varrho''$ die γ Zahlen der Gruppe $-r$ und endlich $-i\varrho'''$ die δ Zahlen aus der Gruppe $-ir$, denen die Zahlen $n.r$ congruent werden, sodass die Zahlen $\varrho, \varrho', \varrho'', \varrho'''$ sämmtlich der Gruppe r angehören, so wird

$$(10) \qquad n^{\frac{\mu-1}{4}}.\Pi(r) \equiv i^{\beta+2\gamma+3\delta}.\Pi(\varrho).\Pi(\varrho').\Pi(\varrho'').\Pi(\varrho''') \pmod{m},$$

wo die Zeichen Π die Producte aller gleichartigen Zahlen bezeichnen. Nun erfüllen aber die Zahlen $\varrho, \varrho', \varrho'', \varrho'''$ die ganze Gruppe r, sodass die Producte beiderseits gleich und, weil ihre Factoren zu m prim sind, wegzuheben sind. Denn, weil die $\frac{\mu-1}{4}$ Zahlen $n \,.\, r$ unter einander incongruent sind, gilt dasselbe von je zwei Zahlen, welche derselben der vier Classen $\varrho, \varrho', \varrho'', \varrho'''$ angehören. Aber es können auch nicht zwei Zahlen aus verschiedenen dieser Classen congruent sein; wäre nämlich z. B., wenn $nr' \equiv i\varrho'$, $nr'' \equiv -\varrho''$ (mod. m) gesetzt wird, $\varrho' \equiv \varrho''$, so ergäbe sich $n\,(r' + ir'') \equiv 0$ (mod. m), also $r' \equiv -ir''$ (mod. m), gegen die Zusammensetzung unseres Restensystems. Nach der hiernach zulässigen Division mit dem Producte $\Pi(r)$ nimmt die Congruenz (10) die Form an:

$$n^{\frac{\mu-1}{4}} \equiv i^{\beta+2\gamma+3\delta} \pmod{m}$$

und liefert durch Vergleichung mit der Congruenz (7) die Gleichung (9).

9. Das Symbol $\left(\left(\frac{n}{m}\right)\right)$ gehorcht folgenden einfachen Gesetzen:

Da zwei congruente Zahlen offenbar gleichen biquadratischen Character haben, so ist:

$$(11) \qquad \left(\left(\frac{n'}{m}\right)\right) = \left(\left(\frac{n}{m}\right)\right), \text{ wenn } n' \equiv n \pmod{m} \text{ ist.}$$

Sind n, n' zwei gleiche oder verschiedene, durch m nicht theilbare ganze complexe Zahlen, so folgt aus den Congruenzen:

$$n^{\frac{\mu-1}{4}} \equiv \left(\left(\frac{n}{m}\right)\right), \quad n'^{\frac{\mu-1}{4}} \equiv \left(\left(\frac{n'}{m}\right)\right) \pmod{m}$$

die dritte:

$$(nn')^{\frac{\mu-1}{4}} \equiv \left(\left(\frac{n}{m}\right)\right) \cdot \left(\left(\frac{n'}{m}\right)\right)$$

und daraus mit Leichtigkeit die Gleichung:

$$(12) \qquad \left(\left(\frac{nn'}{m}\right)\right) = \left(\left(\frac{n}{m}\right)\right) \cdot \left(\left(\frac{n'}{m}\right)\right).$$

Da hiernach der biquadratische Character eines Productes durch die Charactere seiner Factoren bestimmt wird, so kann man sich im Folgenden auf die Betrachtung der einfachen Fälle:

$$n = i, \; n = 1 + i, \; n = m',$$

worin m' eine von m verschiedene ungerade complexe Primzahl ist, beschränken, weil aus diesen Zahlen jede andere durch m nicht theilbare durch Multiplication zusammengesetzt werden kann. Es bleiben mit andern Worten folgende drei Symbole zu bestimmen:

$$\left(\left(\frac{i}{m}\right)\right), \; \left(\left(\frac{1+i}{m}\right)\right), \; \left(\left(\frac{m'}{m}\right)\right).$$

Das erste derselben ist leicht anzugeben, denn nach der Definition selbst ist

$$\left(\left(\frac{i}{m}\right)\right) = i^{\frac{\mu-1}{4}}.$$

Es sei nun zuerst $m = q$, so findet sich hieraus

$$\left(\left(\frac{i}{q}\right)\right) = i^{\frac{q^2-1}{4}}.$$

Wenn zweitens $m = a + bi$ und $p = a^2 + b^2$ ist, so ergiebt sich

$$\left(\left(\frac{i}{a+bi}\right)\right) = i^{\frac{p-1}{4}}.$$

Wir wollen $a + bi$ primär annehmen, also entweder $a = 4k + 1$ $b = 4l$, in welchem Falle $i^{\frac{a^2+b^2-1}{4}} = i^{2k}$ wird, welches auch gleich $i^{3.\frac{a-1}{2}}$ gesetzt werden kann; oder $a = 4k + 3$, $b = 4l + 2$, wo dann $i^{\frac{a^2+b^2-1}{4}} = i^{6k+3} = i^{3.\frac{a-1}{2}}$ wird. Beachtet man, dass q negativ zu nehmen ist, um eine primäre complexe Zahl zu werden, und dass für $a = -q$

$$i^{3.\frac{a-1}{2}} = i^{\frac{q^2-1}{4}}$$

wird, nämlich $+1$, wenn $q = 8h + 7$, gleich -1, wenn $q = 8h + 3$ ist, so findet man den Satz:

Bedeutet $a + bi$ eine (eingliedrige oder zweigliedrige) primäre Primzahl, so ist stets

$$(13) \qquad \left(\left(\frac{i}{a+bi}\right)\right) = i^{3.\frac{a-1}{2}}.$$

Hiernach gehört i zu den Classen 1, 2, 3, 4, jenachdem a die Formen $8k + 1$, $8k + 7$, $8k + 5$, $8k + 3$ hat.

Das Symbol $\left(\left(\frac{1+i}{m}\right)\right)$ soll später in einem besonderen Ergänzungssatze bestimmt werden, für das dritte Symbol existirt wieder ein eigenthümliches Reciprocitätsgesetz, welches sogleich mittels der Kreistheilung bewiesen werden soll. Es wird aber gut sein, noch ein Paar vorläufige Betrachtungen hier anzuschliessen.

10. Jacobi hat eine Verallgemeinerung des Legendre'schen Zeichens in die Theorie der quadratischen Reste eingeführt,*) welche auch auf das Symbol, das den biquadratischen Character bezeichnet, mit Vortheil zum Beweise des Reciprocitätsgesetzes Anwendung findet. Ist nämlich m irgend eine zusammengesetzte

*) In der Note über die Kreistheilung.

ungerade complexe Zahl, etwa

$$m = i^\alpha \,.\, \Pi(q) \,.\, \Pi(\varpi),$$

worin i^α eine complexe Einheit, $\Pi(q)$ das Product von beliebig viel reellen Primzahlen von der Form $4n + 3$, $\Pi(\varpi)$ aber das Product von beliebig viel zweigliedrigen complexen Primzahlen bezeichnet, und ist n irgend welche zu m prime complexe Zahl, so wollen wir das Symbol $\left(\left(\frac{n}{m}\right)\right)$ durch folgende Gleichung definiren:

$$(14) \qquad \left(\left(\frac{n}{m}\right)\right) = \Pi\left(\left(\frac{n}{q}\right)\right) \cdot \Pi\left(\left(\frac{n}{\varpi}\right)\right),$$

in welcher zur Rechten die Symbole die frühere Bedeutung haben, die Producte aber sich resp. auf alle jene Primzahlen q, ϖ erstrecken.

Dies allgemeine Symbol gehorcht denselben Gesetzen, wie das frühere. In der That, es ist erstens

$$(15) \qquad \left(\left(\frac{n'}{m}\right)\right) = \left(\left(\frac{n}{m}\right)\right), \text{ wenn } n' \equiv n \pmod{m}.$$

Denn, da die Congruenz auch für jeden der Moduln q und ϖ besteht, so ist

$$\left(\left(\frac{n'}{q}\right)\right) = \left(\left(\frac{n}{q}\right)\right), \quad \left(\left(\frac{n'}{\varpi}\right)\right) = \left(\left(\frac{n}{\varpi}\right)\right),$$

woraus nach der Definitionsgleichung sich das Behauptete ergiebt. Zweitens ist auch

$$(16) \qquad \left(\left(\frac{nn'}{m}\right)\right) = \left(\left(\frac{n}{m}\right)\right) \cdot \left(\left(\frac{n'}{m}\right)\right),$$

da nach der Gleichung (12) sowohl

$$\left(\left(\frac{nn'}{q}\right)\right) = \left(\left(\frac{n}{q}\right)\right) \cdot \left(\left(\frac{n'}{q}\right)\right)$$

als auch

$$\left(\left(\frac{nn'}{\varpi}\right)\right) = \left(\left(\frac{n}{\varpi}\right)\right) \cdot \left(\left(\frac{n'}{\varpi}\right)\right)$$

ist.

Eine andere nützliche Bemerkung ist folgende: Ist $\alpha + \beta i$ eine nicht durch die ungerade complexe Primzahl $a + bi$ theilbare Zahl, so besteht die Beziehung:

$$(17) \qquad \left(\left(\frac{\alpha - \beta i}{a - bi}\right)\right) = \left(\left(\frac{\alpha + \beta i}{a + bi}\right)\right)^3.$$

Denn, ist i^ϱ der Werth des Symbols $\left(\left(\frac{\alpha+\beta i}{a+bi}\right)\right)$, so ist nach der Definition:

$$(\alpha+\beta i)^{\frac{\mu-1}{4}} \equiv i^\varrho \quad \text{mod.}\ (a+bi),$$

wenn $\mu = N\,(a+bi)$; diese Congruenz kann man auch, durch $A+Bi$ eine gewisse complexe ganze Zahl bezeichnend, als Gleichung so schreiben:

$$(\alpha+\beta i)^{\frac{\mu-1}{4}} = i^\varrho + (a+bi)\,(A+Bi),$$

woraus sich durch Vertauschung von i mit $-i$ folgende Gleichung:

$$(\alpha-\beta i)^{\frac{\mu-1}{4}} = i^{3\varrho} + (a-bi)\,(A-Bi)$$

d. h. die Congruenz

$$(\alpha-\beta i)^{\frac{\mu-1}{4}} \equiv i^{3\varrho} \ \text{mod.}\ (a-bi)$$

und folglich die Gleichung (17) ergiebt. — Dieser Satz lässt sich offenbar sogleich vermittelst der Gleichung (14) auf zwei relative Primzahlen $\alpha+\beta i$, $a+bi$ erweitern, von denen die zweite ungerade ist.

Jetzt bezeichne n eine reelle Zahl, welche durch eine Primzahl q von der Form $4n+3$ nicht theilbar ist. Da nach dem Fermat'schen Lehrsatze $n^{q-1} \equiv 1$ (mod. q) und $\frac{q+1}{4}$ eine ganze Zahl ist, findet sich durch Erhebung der Congruenz in die $\frac{q+1}{4}$te Potenz: $n^{\frac{q^2-1}{4}} \equiv 1$ (mod. q), folglich

$$\left(\left(\frac{n}{q}\right)\right) = +1\,.$$

Ist dagegen p eine, nicht in n aufgehende reelle Primzahl von der Form $4m+1$, und ϖ, ϖ' ihre beiden conjugirt-complexen Factoren, so folgt aus Gleichung (17):

$$\left(\left(\frac{n}{\varpi'}\right)\right) = \left(\left(\frac{n}{\varpi}\right)\right)^3, \text{ also } \left(\left(\frac{n}{p}\right)\right) = \left(\left(\frac{n}{\varpi}\right)\right)\cdot\left(\left(\frac{n}{\varpi'}\right)\right) = \left(\left(\frac{n}{\varpi}\right)\right)^4 = 1\,.$$

Jede ungerade reelle Zahl m kann nun unter der Form

$$\pm\, \Pi(q)\,.\,\Pi(p) = \pm\, \Pi(q)\,.\,\Pi\,(\varpi\varpi')$$

gedacht, nämlich in eine gewisse Anzahl ungerader reeller Primzahlen zerlegt werden, von denen die einen von der Art $q = 4n+3$,

die andern von der Art $p = 4n + 1$, also als Product aus zwei conjugirt-complexen Primzahlen ϖ und ϖ' darstellbar sind. Verbindet man daher die beiden vorher erhaltenen Resultate mit der Gleichung (14), so ergiebt sich der Satz: **Sind** m, n **zwei reelle relative Primzahlen, deren erstere ungerade ist, so ist stets:**

$$\left(\left(\frac{n}{m}\right)\right) = +1. \tag{18}$$

Endlich bemerken wir, dass nach Gleichung (17)

$$\left(\left(\frac{i}{\varpi'}\right)\right) = \left(\left(\frac{-i}{\varpi}\right)\right)^3, \text{ also } \left(\left(\frac{i}{p}\right)\right) = \left(\left(\frac{-1}{\varpi}\right)\right) = (-1)^{\frac{p-1}{4}}$$

ist, wofür man auch $(-1)^{\frac{p^2-1}{8}}$ setzen kann, da p von der Form $4n + 1$ ist; in der That, für $p = 8n + 1$ werden die Exponenten $\frac{p-1}{4}$ und $\frac{p^2-1}{8}$ gleichzeitig gerade, für $p = 8n + 5$ gleichzeitig ungerade sein. Andererseits ist

$$\left(\left(\frac{i}{q}\right)\right) = i^{\frac{q^2-1}{4}} = (-1)^{\frac{q^2-1}{8}}.$$

Ist also m eine ungerade reelle Zahl, sodass wir setzen können

$$m = \pm \Pi(p) . \Pi(q),$$

so ergiebt sich nach (14) die Gleichung

$$\left(\left(\frac{i}{m}\right)\right) = (-1)^{\Sigma\frac{q^2-1}{8} + \Sigma\frac{p^2-1}{8}}. \tag{19}$$

Indem man nun m^2 unter folgender Form schreibt:

$$m^2 = \Pi(1 + (q^2 - 1)) . \Pi(1 + (p^2 - 1))$$

und beachtet, dass jede der Differenzen $q^2 - 1$, $p^2 - 1$ durch 8 theilbar, also nach Entwicklung des Productes

$$m^2 \equiv 1 + \Sigma(q^2 - 1) + \Sigma(p^2 - 1) \pmod{64}$$

ist, findet man

$$\frac{m^2-1}{8} \equiv \sum\frac{q^2-1}{8} + \sum\frac{p^2-1}{8} \pmod{2},$$

kann also die Gleichung (19) auch folgendermassen schreiben:

$$\left(\left(\frac{i}{m}\right)\right) = (-1)^{\frac{m^2-1}{8}}. \tag{20}$$

Dreizehnte Vorlesung.

Das Reciprocitätsgesetz der biquadratischen Reste.

1. Um das Reciprocitätsgesetz für die biquadratischen Reste zu erhalten, bedienen wir uns ganz ähnlicher Mittel, wie bei dem Beweise des quadratischen Reciprocitätsgesetzes. Wir nehmen an, p sei eine reelle Primzahl von der Form $4n+1$, und gehen dann aus von der Formel:

$$(\omega^h, r) = \sum_{\mu=1}^{\mu=p-1} \omega^{h\,\mathrm{ind}.\mu} . r^\mu = \sum_{\lambda=0}^{\lambda=p-2} \omega^{h\lambda} . r^{g^\lambda}.$$

Setzen wir darin successive h gleich $\frac{p-1}{4}, 2.\frac{p-1}{4}, 3.\frac{p-1}{4}$, wobei $\omega^{\frac{p-1}{4}} = i$ wird, so erhalten wir die drei Ausdrücke:

$$(1) \qquad (i, r) = \sum_{\lambda=0}^{\lambda=p-2} i^\lambda . r^{g^\lambda}, \quad (-1, r) = \sum_{\lambda=0}^{\lambda=p-2} i^{2\lambda} . r^{g^\lambda},$$

$$(-i, r) = \sum_{\lambda=0}^{\lambda=p-2} i^{3\lambda} . r^{g^\lambda},$$

welche wir kurz durch S_1, S_2, S_3 resp. bezeichnen wollen. Der zweite derselben ist kein anderer, als der in Nr. 3 der 9. Vorlesung mit S bezeichnete; denn für jeden geraden Werth des λ ist $i^{2\lambda} = +1$ und g^λ quadratischer Rest, für jedes ungerade λ dagegen ist $i^{2\lambda} = -1$ und g^λ quadratischer Nichtrest von p, d. h.

$$\sum_{\lambda=0}^{\lambda=p-2} i^{2\lambda} . r^{g^\lambda} = \sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right) . r^s .$$

Nach Formel (25) ebendaselbst erhält man also für den hier vorliegenden Fall:

$$(2) \qquad S_2 = +\sqrt{p}\,.$$

Wenn man nun auch in den Formeln (34) und (29) der 8. Vorlesung, von der Voraussetzung $h = \frac{p-1}{4}$ ausgehend, $\alpha = \omega^{\frac{p-1}{4}} = i$, $e = 4$ setzt, so nehmen sie die Gestalt an:

$$(3) \qquad (i, r)^4 = (-1)^{\frac{p-1}{4}} . p\, \psi_1(i)\, \psi_2(i)$$

$$(4) \qquad (i, r)\,(-i, r) = (-1)^{\frac{p-1}{4}} . p\,.$$

Die Ausdrücke von $\psi_1(i)$ und $\psi_2(i)$ aber haben wir bereits in Nr. 4 der 10. Vorlesung gefunden, nämlich

$$(5) \qquad \psi_1(i) = \frac{(i, r)^2}{(-1, r)}, \quad \psi_2(i) = \frac{(i, r) \cdot (-1, r)}{(-i, r)},$$

und zwischen ihnen die Beziehung

$$(6) \qquad \psi_2(i) = (-1)^{\frac{p-1}{4}} \cdot \psi_1(i) .$$

Beachtet man endlich, dass

$$\psi_2(i) = \sum_{\mu=1}^{\mu=p-2} i^{\text{ind.}\mu + \text{ind.}(1+\mu)}$$

also nach Nr. 3 derselben Vorlesung gleich einem complexen Factor $a + bi$ der Primzahl p war, und substituirt Alles in die Gleichung (3), so ergiebt sich:

$$(7) \qquad (i, r)^4 = p \cdot (a + bi)^2,$$

und wegen (4):

$$(8) \qquad (-i, r)^4 = p \cdot (a - bi)^2 .$$

Nach dem Hauptsatze am Schlusse von Nr. 3 der vorigen Vorlesung ist eine Primzahl p nur auf eine Art in zwei primäre conjugirt complexe Factoren zerlegbar. Da wir nun vermittelst der Kreistheilung die Zerlegung

$$p = (a + bi)(a - bi)$$

gefunden haben, so entsteht hier die Frage, ob die Factoren $a + bi$, $a - bi$ primär sind oder nicht, und wenn das Letztere, in welcher Beziehung sie zu den primären Factoren von p stehen. Obwohl die Mittel zur Entscheidung dieser Frage durch Nr. 5 der 10. Vorlesung bereits gewonnen worden sind, möge es gestattet sein, aus Jacobi's Vorlesungen über Zahlentheorie noch eine andere interessante Methode zu ihrer Beantwortung hier mitzutheilen.

2. Aus der ersten der Gleichungen (5) ergiebt sich mit Rücksicht auf (6):

$$(9) \qquad S_1^2 = (-1)^{\frac{p-1}{4}} \cdot (a + bi) \cdot S_2$$

und folglich wegen der Gleichungen

$$S_1 \cdot S_3 = (i, r) \cdot (-i, r) = (-1)^{\frac{p-1}{4}} \cdot (a^2 + b^2) \text{ und } S_2 = \sqrt{p}$$

auch:

(10) $$S_3^2 = (-1)^{\frac{p-1}{4}} . (a - bi) . S_2 .$$

Wenn man nun wieder, wie in Nr. 3 der 9. Vorlesung

$$U = \sum_{\alpha} r^{\alpha} = \sum_{h=0}^{h=\frac{p-3}{2}} r^{g^{2h}}, \quad V = \sum_{\beta} r^{\beta} = \sum_{h=0}^{h=\frac{p-3}{2}} r^{g^{2h+1}}$$

setzt, sodass $U = \frac{-1 + \sqrt{p}}{2}$ wird, so findet man

(11) $$U^2 - \left(\frac{S_1 + S_3}{2}\right)^2 = \left(\sum_{h=0}^{h=\frac{p-3}{2}} r^{g^{2h}}\right)^2 - \left(\sum_{h=0}^{h=\frac{p-3}{2}} (-1)^h . r^{g^{2h}}\right)^2,$$

denn in dem Ausdrucke

$$S_1 + S_3 = \sum_{h=0}^{h=p-2} (i^h + i^{3h})\, r^{g^h}$$

kann man die geraden Werthe des h und die ungeraden unterscheiden, letztere machen den Coëfficienten $i^h + i^{3h}$ zu Null, erstere zu $+ 2$, wenn h durch 4 theilbar ist, und zu $- 2$, wenn $h \equiv 2$ (mod. 4) ist; daraus ergiebt sich die Richtigkeit obiger Formel. Nun kann man einerseits in der rechten Seite derselben die Quadrate nach dem binomischen Lehrsatze entwickeln, wobei man sich leicht überzeugt, dass alle Glieder, welche sich nicht fortheben, durch 4 theilbare Coëfficienten haben, sodass man die rechte Seite gleich $4 . f(r)$ setzen kann, wo $f(r)$ eine ganze und ganzzahlige Function von r ist, deren Grad man vermittelst der Gleichung

$$r^{p-1} + r^{p-2} + \ldots . + r + 1 = 0$$

unter den $(p - 1)^{ten}$ erniedrigt annehmen darf. Andrerseits erhält man, da

$$(S_1 + S_3)^2 = S_1^2 + S_3^2 + 2 . S_1 . S_3$$

d. h. nach den Formeln (4), (9) und (10)

$$(S_1 + S_3)^2 = 2a . (-1)^{\frac{p-1}{4}} S_2 + 2 . (-1)^{\frac{p-1}{4}} p$$

ist, für die linke Seite jener Formel den Werth:

$$\left(\frac{p+1}{4} - \frac{(-1)^{\frac{p-1}{4}} . p}{2}\right) - \frac{a\,(-1)^{\frac{p-1}{4}} + 1}{2} . S_2 .$$

Dieser nimmt aber, da $S_2 = U - V$ vermittelst der Gleichung $1 + U + V = 0$ sich auch $S_2 = -1 - 2V$ schreiben lässt, folgende Form an:

$$\left(\frac{p+1}{4} + \frac{(-1)^{\frac{p-1}{4}}.a+1}{2} - \frac{(-1)^{\frac{p-1}{4}}.p}{2}\right) + \left((-1)^{\frac{p-1}{4}}.a+1\right).\sum_{\beta} r^{\beta}$$

und enthält nur kleinere Potenzen von r, als die $(p-1)^{te}$, da $p-1$ quadratischer Rest von p, also nicht unter den Nichtresten β aus der Reihe $1, 2, 3, \ldots . p-1$ befindlich ist. Da nun beide Seiten der so reducirten Formel (11) wegen der Irreductibilität der Kreistheilungsgleichung identisch gleich sein müssen, so ergiebt sich das Resultat, dass $(-1)^{\frac{p-1}{4}}.a + 1 \equiv 0$ (mod. 4) sein muss; also erhält a die Form $4n - 1$, wenn p die Form $8m + 1$ hat, dagegen die Form $4n + 1$, wenn p von der Form $8m + 5$ ist. Dies ist genau der in Nr. 5 der 10. Vorlesung gefundene Satz.

3. Aus dieser Untersuchung geht hervor, dass die complexen Factoren $a + bi$, in welche die Kreistheilung die Zahl p zerlegt, nicht primär sind, sondern, um es zu werden, negativ genommen werden müssen. In der That, da das Quadrat jeder ungeraden Zahl congruent Eins ist (mod. 8), so muss, wie leicht zu übersehen ist, b durch 4 theilbar sein, wenn $p = a^2 + b^2$ die Form $8n + 1$ hat. Dagegen muss b die Form $4m + 2$ haben, wenn p von der Form $8n + 5$ ist. In dem ersten Falle findet sich also aus der Kreistheilung $a + bi \equiv -1$ (mod. 4), folglich $-(a + bi) \equiv +1$ (mod. 4) d. h. primär; in dem zweiten Falle ist $a + bi \equiv 1 + 2i$ (mod. 4), folglich $-(a + bi) \equiv 3 + 2i$ (mod. 4), also wieder primär.

Wenn hiernach ϖ, ϖ' die beiden conjugirten primären Factoren von p sind, so ist $-(a + bi)$ einem derselben gleich, und zwar kann man es nach Belieben etwa gleich ϖ voraussetzen, wenn man die primitive Wurzel passend wählt; denn wir wissen aus Nr. 6 der angeführten Vorlesung, dass das Zeichen von b mit der Wahl der primitiven Wurzel g wechselt. Bei solcher Wahl der primitiven Wurzel g folgt aber aus den beiden Congruenzen:

$$a + b \cdot g^{\frac{p-1}{4}} \equiv 0, \quad a + bi \equiv 0 \pmod{\varpi},$$

deren erstere nach Formel (23) derselben Vorlesung sogar (mod. p) erfüllt ist, die Congruenz

$$g^{\frac{p-1}{4}} \equiv i \pmod{\varpi},$$

und diese gestattet, den Ausdrücken S_1, S_2, S_3 eine etwas andere Form zu geben, aus welcher die primitive Wurzel verschwunden ist. In der That, nach der Definition des Symbols für den biquadratischen Character ist wegen der vorigen Congruenz $\left(\left(\frac{g}{\varpi}\right)\right) = i$; indem man dies also für i in S_1 einführt, kommt

$$S_1 = \sum_{\lambda=0}^{\lambda=p-2} \left(\left(\frac{g^\lambda}{\varpi}\right)\right) \cdot r^{g^\lambda}$$

oder, was dasselbe ist,

$$S_1 = \sum_{s=1}^{s=p-1} \left(\left(\frac{s}{\varpi}\right)\right) \cdot r^s \,. \tag{12}$$

Auf dieselbe Weise ergeben sich:

$$S_2 = \sum_{s=1}^{s=p-1} \left(\left(\frac{s}{\varpi}\right)\right)^2 \cdot r^s; \quad S_3 = \sum_{s=1}^{s=p-1} \left(\left(\frac{s}{\varpi}\right)\right)^3 \cdot r^s \,. \tag{13}$$

Ersetzt man in S_1 die Wurzel r durch r^k, während k durch p nicht theilbar ist, und bezeichnet den neuen Werth durch $S_1^{(k)}$, so findet man:

$$S_1^{(k)} = \sum_{s=1}^{s=p-1} \left(\left(\frac{s}{\varpi}\right)\right) \cdot r^{ks} = \left(\left(\frac{k}{\varpi}\right)\right)^3 \cdot \sum_{s=1}^{s=p-1} \left(\left(\frac{ks}{\varpi}\right)\right) \cdot r^{ks}$$

oder vielmehr, da ks gleichzeitig mit s die Reste $1, 2, 3, \ldots p-1$ lässt, wenn auch in anderer Ordnung, und

$$\left(\left(\frac{s'}{\varpi}\right)\right) = \left(\left(\frac{s}{\varpi}\right)\right), \quad r^{s'} = r^s \text{ ist, wenn } s' \equiv s \pmod{p},$$

so wird die einfache Beziehung erhalten:

$$S_1^{(k)} = \left(\left(\frac{k}{\varpi}\right)\right)^3 \cdot S_1 \tag{14}$$

und auf demselben Wege die beiden folgenden, in denen $S_2^{(k)}$, $S_3^{(k)}$ die $S_1^{(k)}$ analoge Bedeutung haben:

$$S_2^{(k)} = \left(\left(\frac{k}{\varpi}\right)\right)^2 \cdot S_2, \quad S_3^{(k)} = \left(\left(\frac{k}{\varpi}\right)\right) \cdot S_3 \,. \tag{15}$$

Endlich ergeben die beiden Formeln (9) und (10) folgende Gleichungen:

$$(16)\quad \begin{cases} \sum_{s=1}^{s=p-1} \left(\left(\frac{s}{\varpi}\right)\right) \cdot r^s = \sqrt{(a+bi)(-1)^{\frac{p-1}{4}}\sqrt{p}} \\ \sum_{s=1}^{s=p-1} \left(\left(\frac{s}{\varpi}\right)\right)^3 \cdot r^s = \sqrt{(a-bi)(-1)^{\frac{p-1}{4}}\sqrt{p}} \end{cases}$$

Während in denselben $\sqrt{p}$ positiv zu nehmen ist, hat man, soviel mir bekannt ist, bisher das Vorzeichen der andern Quadratwurzel noch nicht bestimmt. Für den Beweis des biquadratischen Reciprocitätsgesetzes ist es jedoch ebensowenig wie bei dem des quadratischen nothwendig, dieses Vorzeichen zu kennen, vielmehr reichen die gewonnenen Hilfsformeln in Verbindung mit den Resultaten der vorigen Vorlesung dazu vollständig aus.

4. Bei diesem Beweise unterscheiden wir nun zunächst zwei Fälle: Erstens. Während p stets eine reelle Primzahl von der Form $4n+1$ und ϖ, ϖ' ihre primären complexen Factoren bezeichnen sollen, sei q eine reelle Primzahl von der Form $4n+3$. Erhebt man sodann den Ausdruck S_1 zur q^{ten} Potenz und vernachlässigt alle durch q theilbaren Glieder, so findet man, da offenbar $\left(\left(\frac{s}{\varpi}\right)\right)^q = \left(\left(\frac{s}{\varpi}\right)\right)^3$ ist,

$$S_1{}^q \equiv \sum_{s=1}^{s=p-1} \left(\left(\frac{s}{\varpi}\right)\right)^3 \cdot r^{qs} \pmod{q}$$

d. h. nach den Bezeichnungen und Formeln der vorigen Nummer

$$S_1{}^q \equiv S_3{}^{(q)} \equiv \left(\left(\frac{q}{\varpi}\right)\right) \cdot S_3 \pmod{q}.$$

Multiplicirt man auf beiden Seiten mit S_1 und berücksichtigt die Gleichungen:

$$S_1{}^{q+1} = (S_1{}^4)^{\frac{q+1}{4}} = (p\varpi^2)^{\frac{q+1}{4}},\quad S_1 \cdot S_3 = (-1)^{\frac{p-1}{4}} \cdot p,$$

so ergiebt sich

$$(p\varpi^2)^{\frac{q+1}{4}} \equiv (-1)^{\frac{p-1}{4}} \cdot \left(\left(\frac{q}{\varpi}\right)\right) \cdot p \pmod{q}.$$

Diese Congruenz ist zwar keine gewöhnliche, gestattet aber dieselbe Behandlung, wie eine nur zwischen Zahlen bestehende.

Als Gleichung geschrieben, und wenn die ganze complexe Zahl

$$(p\varpi^2)^{\frac{q+1}{4}} - (-1)^{\frac{p-1}{4}}\left(\left(\frac{q}{\varpi}\right)\right)p$$

gleich $\alpha + \beta i$ gesetzt wird, hat sie nämlich folgende Form:

$$\alpha + \beta i = q \,.\, R,$$

worin R eine ganze Function von r ist, deren Coëfficienten ganze complexe Zahlen sind, sodass man $R = R' + iR''$ setzen kann, wenn unter R', R'' ganze Functionen von r mit reellen Coëfficienten verstanden werden. Nun bleibt jene Gleichung bestehen, wenn in den Coëfficienten i durch $-i$ ersetzt wird, da man die Summe S_3 ähnlich wie S_1 behandeln kann, wodurch man, wie leicht zu übersehen ist,

$$\alpha - \beta i = q\,(R' - iR'')$$

und folglich die beiden Gleichungen erhält:

$$\alpha = q \,.\, R', \;\; \beta = q \,.\, R''.$$

Diese lehren wegen der Irreductibilität der Kreistheilungsgleichung, dass α und β und folglich auch $\alpha + \beta i$ durch q theilbar ist.

Nun ist aber $p = \varpi \,.\, \varpi'$, $(-1)^{\frac{p-1}{4}} = \left(\left(\frac{-1}{\varpi}\right)\right)$ und $\varpi' \equiv \varpi^q$ (mod. q) (s. Nr. 6 der vor. Vorlesung); setzt man dies in die letzte Congruenz ein und dividirt beide Seiten derselben durch ϖ^{q+1}, so findet sich bei Anwendung der letzten Sätze der vor. Vorlesung

$$\varpi^{\frac{q^2-1}{4}} \equiv \left(\left(\frac{-q}{\varpi}\right)\right) \quad (\text{mod. } q),$$

d. h. aber $\left(\left(\frac{\varpi}{q}\right)\right) \equiv \left(\left(\frac{-q}{\varpi}\right)\right)$ (mod. q), oder vielmehr:

$$(17) \qquad \left(\left(\frac{\varpi}{q}\right)\right) = \left(\left(\frac{-q}{\varpi}\right)\right).$$

Diese Gleichung enthält das Reciprocitätsgesetz, welches zwischen einer eingliedrigen und einer zweigliedrigen Primzahl besteht.

Zweitens sei p_1 eine von p verschiedene reelle Primzahl von der Form $4n + 1$ und ϖ_1, ϖ_1' ihre primären complexen Factoren. Die Erhebung des Ausdruckes S_3 in die p_1^{te} Potenz liefert,

wenn alle durch p_1 theilbaren Glieder der Entwicklung vernachlässigt werden, die Congruenz:

$$S_3^{p_1} \equiv \sum_{s=1}^{s=p-1} \left(\left(\frac{s}{\varpi}\right)\right)^{3p_1} \cdot r^{p_1 s} \equiv \sum_{s=1}^{s=p-1} \left(\left(\frac{s}{\varpi}\right)\right)^3 \cdot r^{p_1 s} \pmod{p_1}$$

oder

$$S_3^{p_1} \equiv S_3^{(p_1)} \equiv \left(\left(\frac{p_1}{\varpi}\right)\right) \cdot S_3 \pmod{p_1},$$

also

$$\left[S_3^{p_1-1} - \left(\left(\frac{p_1}{\varpi}\right)\right)\right] \cdot S_3 \equiv 0.$$

Diese Congruenz kann mit Rücksicht auf die Gleichung

$$S_3^{p_1-1} = (S_3^4)^{\frac{p_1-1}{4}} = (p\varpi'^2)^{\frac{p_1-1}{4}}$$

in die Form

$$\left[(p\varpi'^2)^{\frac{p_1-1}{4}} - \left(\left(\frac{p_1}{\varpi}\right)\right)\right] \cdot S_3 \equiv 0 \pmod{p_1}$$

gesetzt werden und geht durch Multiplication mit S_1 in die folgende über:

$$\left[(p\varpi'^2)^{\frac{p_1-1}{4}} - \left(\left(\frac{p_1}{\varpi}\right)\right)\right] \cdot p \equiv 0 \pmod{p_1},$$

auf welche die vorher gemachte Bemerkung Anwendung findet, sodass im gewöhnlichen Sinne die Congruenz

$$(p\varpi'^2)^{\frac{p_1-1}{4}} \equiv \left(\left(\frac{p_1}{\varpi}\right)\right) \pmod{p_1}$$

besteht. Diese bleibt nothwendig auch in Beziehung auf den Factor ϖ_1 von p_1 als Modulus bestehen und liefert dann

$$\left(\left(\frac{p\varpi'^2}{\varpi_1}\right)\right) = \left(\left(\frac{\varpi}{\varpi_1}\right)\right) \cdot \left(\left(\frac{\varpi'}{\varpi_1}\right)\right)^3 \equiv \left(\left(\frac{p_1}{\varpi}\right)\right) \pmod{\varpi_1},$$

folglich die Gleichung:

$$\left(\left(\frac{\varpi}{\varpi_1}\right)\right) \cdot \left(\left(\frac{\varpi'}{\varpi_1}\right)\right)^3 = \left(\left(\frac{p_1}{\varpi}\right)\right).$$

Nach Nr. 10 der vor. Vorlesung ist endlich

$$\left(\left(\frac{\varpi'}{\varpi_1}\right)\right)^3 = \left(\left(\frac{\varpi}{\varpi_1'}\right)\right) \text{ und } \left(\left(\frac{\varpi}{\varpi_1}\right)\right) \cdot \left(\left(\frac{\varpi}{\varpi_1'}\right)\right) = \left(\left(\frac{\varpi}{p_1}\right)\right);$$

demnach findet man:

$$\left(\left(\frac{\varpi}{p_1}\right)\right) = \left(\left(\frac{p_1}{\varpi}\right)\right). \tag{18}$$

5. Aus den beiden Gleichungen (17) und (18) lässt sich ein allgemeineres Resultat ableiten, welches in Verbindung mit den letzten Formeln der vorigen Vorlesung das zwischen zwei zweigliedrigen Primzahlen bestehende Reciprocitätsgesetz ergeben wird. Es bezeichne m irgend eine ungerade, positive oder negative reelle Zahl, welche aber mit Rücksicht auf das Vorzeichen die Form $4n+1$ hat, und M eine complexe gegen m prime Zahl, in welcher der reelle Theil ungerade, der Coëfficient von i aber gerade ist, so wird behauptet, es sei stets:

$$\left(\left(\frac{m}{M}\right)\right) = \left(\left(\frac{M}{m}\right)\right). \tag{19}$$

In der That, da eine solche Zahl M nach Nr. 2, 4) der vor. Vorlesung den Factor $1+i$ nicht enthält, kann man

$$M = \pm\, \Pi(q)\,.\,\Pi(\varpi)$$

setzen, indem das erste Product alle reellen Primzahlen von M, welche die Form $4n+3$ haben, das zweite alle zweigliedrigen Primfactoren von M enthält. Da andererseits m, wenn es die Form $4n+1$ haben soll, positiv oder negativ sein muss, jenachdem die Anzahl seiner Primfactoren von der Form $4n+3$ gerade oder ungerade ist, so wird man es stets in die Form

$$m = \Pi(-q_1)\,.\,\Pi(p_1)$$

bringen können, in welcher das zweite Product alle Primfactoren von m, welche die Form $4n+1$, das erste alle diejenigen enthält, welche die Form $4n+3$ haben, jeden der letztern mit negativem Vorzeichen, d. h. primär genommen. Hiernach ergiebt sich aus Formel (12) der vor. Vorlesung, da nach (18) ebend. $\left(\left(\frac{\pm 1}{m}\right)\right) = +1$ ist,

$$\left(\left(\frac{M}{m}\right)\right) = \prod\left(\left(\frac{q}{m}\right)\right)\cdot\prod\left(\left(\frac{\varpi}{m}\right)\right),$$

das erste Product auf alle q, das zweite auf alle ϖ bezogen, und weiter nach Formel (14) ebendaselbst:

$$\left(\left(\frac{M}{m}\right)\right) = \prod\left(\left(\frac{q}{q_1}\right)\right)\cdot\prod\left(\left(\frac{q}{p_1}\right)\right)\cdot\prod\left(\left(\frac{\varpi}{q_1}\right)\right)\cdot\prod\left(\left(\frac{\varpi}{p_1}\right)\right).$$

wo die einzelnen Producte sich stets auf alle Combinationen der darin angedeuteten Zahlclassen beziehen, z. B. in dem ersten jede der Primzahlen q mit jeder der Primzahlen q_1 zu combiniren

und das Product der entstehenden Symbole zu bilden ist. — Die Symbole in den beiden ersten Producten können ohne Weiteres in $\left(\left(\frac{-q_1}{q}\right)\right)$ und $\left(\left(\frac{p_1}{q}\right)\right)$ umgekehrt werden, da sie, ebenso wie die umgekehrten Symbole, auf zwei reelle Zahlen bezüglich, also nach Gleichung (18) der vor. Vorlesung der Einheit gleich sind. Die Symbole des dritten Products können nach Formel (17) in $\left(\left(\frac{-q_1}{\varpi}\right)\right)$, die des vierten nach Formel (18) in $\left(\left(\frac{p_1}{\varpi}\right)\right)$ verkehrt werden, so dass sich ergiebt:

$$\left(\left(\frac{M}{m}\right)\right)=\Pi\left(\left(\frac{-q_1}{q}\right)\right)\cdot\Pi\left(\left(\frac{p_1}{q}\right)\right)\cdot\Pi\left(\left(\frac{-q_1}{\varpi}\right)\right)\cdot\Pi\left(\left(\frac{p_1}{\varpi}\right)\right)$$

oder

$$\left(\left(\frac{M}{m}\right)\right)=\Pi\left(\left(\frac{m}{q}\right)\right)\cdot\Pi\left(\left(\frac{m}{\varpi}\right)\right),$$

wo das erste Product auf alle q, das zweite auf alle ϖ zu erstrecken ist, oder endlich nach Formel (14) vor. Vorlesung, wie behauptet wurde,

$$\left(\left(\frac{M}{m}\right)\right)=\left(\left(\frac{m}{M}\right)\right).$$

6. Nun mögen $a+bi$ und $\alpha+\beta i$ zwei primäre zweigliedrige Primzahlen bezeichnen. Aus der identischen Gleichung

$$\alpha(a+bi)=a\alpha+b\beta+bi(\alpha+\beta i),$$

welche als Congruenz folgendermassen geschrieben werden kann:

$$\alpha(a+bi)\equiv a\alpha+b\beta \mod.(\alpha+\beta i),$$

ergiebt sich nach den Formeln (15) und (16) der vor. Vorlesung die Gleichung

$$\left(\left(\frac{\alpha}{\alpha+\beta i}\right)\right)\cdot\left(\left(\frac{a+bi}{\alpha+\beta i}\right)\right)=\left(\left(\frac{a\alpha+b\beta}{\alpha+\beta i}\right)\right)$$

und auf ähnlichem Wege die folgende:

$$\left(\left(\frac{a}{a+bi}\right)\right)\cdot\left(\left(\frac{\alpha+\beta i}{a+bi}\right)\right)=\left(\left(\frac{a\alpha+b\beta}{a+bi}\right)\right),$$

welche wir in die dritte Potenz erheben und mit der vorigen multipliciren wollen. Beachtet man dabei die Gleichung (17) der vor. Vorlesung und, dass die 4[te] Potenz des biquadratischen Symbols stets gleich der Einheit ist, so giebt man der resultirenden

Gleichung leicht die Form:

$$(20)\qquad \left(\left(\frac{a+bi}{\alpha+\beta i}\right)\right)\cdot\left(\left(\frac{\alpha+\beta i}{a+bi}\right)\right)^3$$
$$=\left(\left(\frac{\alpha}{\alpha+\beta i}\right)\right)^3\cdot\left(\left(\frac{a}{a+bi}\right)\right)\cdot\left(\left(\frac{a\alpha+b\beta}{(a-bi)(\alpha+\beta i)}\right)\right).$$

Nun bezeichne e die Einheit, mit solchem Vorzeichen genommen, dass $ae \equiv 1 \pmod{4}$ wird, ebenso ε diejenige Einheit, welche der Congruenz $\alpha\varepsilon \equiv 1 \pmod{4}$ genügt, so dass auch $a\alpha\,.\,e\varepsilon \equiv 1$ oder, was dasselbe ist, da b, β gerade, also $b\beta \equiv 0 \pmod{4}$ ist, dass $e\varepsilon(a\alpha+b\beta) \equiv 1 \pmod{4}$ wird. Dann ist es leicht, die rechte Seite der obigen Gleichung in folgende Form zu bringen:

$$\left(\left(\frac{\alpha\varepsilon}{\alpha+\beta i}\right)\right)^3\cdot\left(\left(\frac{ae}{a+bi}\right)\right)\cdot\left(\left(\frac{(a\alpha+b\beta)\,e\varepsilon}{a\alpha+b\beta+i(a\beta-\alpha b)}\right)\right)$$
$$\cdot\left(\left(\frac{\varepsilon}{a+bi}\right)\right)\cdot\left(\left(\frac{e}{\alpha-\beta i}\right)\right).$$

In diesem Ausdrucke können die drei ersten Symbole nach Formel (19) umgekehrt werden und erhalten mit Rücksicht auf die Formeln (14) und (18) der vor. Vorlesung die Werthe:

$$\left(\left(\frac{i}{\alpha}\right)\right),\quad\left(\left(\frac{i}{a}\right)\right),\quad\left(\left(\frac{i}{a\alpha+b\beta}\right)\right),$$

deren Product nach Formel (20) ebendas. sich gleich

$$(-1)^{\frac{a^2\alpha^2-1+ab\alpha\beta}{4}+\frac{b^2\beta^2}{8}}$$

ergiebt. Da nun $a\alpha$ ungerade, $b\beta$ durch 4 theilbar ist, so findet man leicht, dass der Exponent dieser Potenz $\equiv \frac{b\beta}{4} \pmod{2}$, die Potenz selbst also gleich $(-1)^{\frac{b\beta}{4}}$ ist.

Untersuchen wir noch das Product der beiden letzten Symbole. Diese haben aber resp. die Werthe $\varepsilon^{\frac{p-1}{4}}$ und $e^{\frac{p_1-1}{4}}$, wo $p=a^2+b^2$, $p_1=\alpha^2+\beta^2$ gesetzt ist. Unterscheiden wir nun zwei Fälle: In dem ersten Falle ist $e=\varepsilon$, also $a\alpha \equiv 1 \pmod{4}$, woraus folgt, dass entweder a, α Beide die Form $4n+1$ und folglich, da $a+bi$, $\alpha+\beta i$ primär vorausgesetzt sind, p, p_1 Beide die Form $8n+1$ haben, was

$$\varepsilon^{\frac{p-1}{4}}\,.\,e^{\frac{p_1-1}{4}}=\varepsilon^{\frac{p-1}{4}+\frac{p_1-1}{4}}=+1$$

ergeben würde; oder a, α müssen Beide die Form $4n+3$, folglich p, p_1 Beide die Form $8n+5$ haben, wo dann wieder

$$\varepsilon^{\frac{p-1}{4}} \cdot e^{\frac{p_1-1}{4}} = \varepsilon^{\frac{p-1}{4}+\frac{p_1-1}{4}} = +1$$

sich ergiebt. — In dem zweiten Falle ist $e = -\varepsilon$, also $a\alpha \equiv 3 \pmod{4}$; demnach muss eine der beiden Zahlen a, α, z. B. α die Form $4n+3$, die andere, z. B. a, die Form $4n+1$ haben, dem entsprechend würde $e = 1$, $\varepsilon = -1$, p von der Form $8n+1$, p_1 von der Form $8n+5$ und

$$\varepsilon^{\frac{p-1}{4}} \cdot e^{\frac{p_1-1}{4}} = (-1)^{\frac{p-1}{4}} = +1$$

sein. — Allgemein hat daher das Product der beiden letzten Symbole den Werth $+1$, und man findet endlich:

$$\left(\left(\frac{a+bi}{\alpha+\beta i}\right)\right) \cdot \left(\left(\frac{\alpha+\beta i}{a+bi}\right)\right)^3 = (-1)^{\frac{b\beta}{4}}$$

oder

$$(21) \qquad \left(\left(\frac{a+bi}{\alpha+\beta i}\right)\right) = \left(\left(\frac{\alpha+\beta i}{a+bi}\right)\right) \cdot (-1)^{\frac{b\beta}{4}}.$$

Diese Formel enthält das Reciprocitätsgesetz für zwei zweigliedrige primäre Primzahlen.

Bedeuten endlich q, q_1 zwei reelle Primzahlen von der Form $4n+3$, so ist wegen der Formel (18) der vor. Vorlesung offenbar:

$$(22) \qquad \left(\left(\frac{-q}{q_1}\right)\right) = \left(\left(\frac{-q_1}{q}\right)\right)$$

und die Formeln (17), (21), (22) umfassen alle nur möglichen Fälle. Sie lassen sich in eine einzige zusammenfassen vermittelst folgender Betrachtung: Da $p = a^2 + b^2$, $p_1 = \alpha^2 + \beta^2$ gesetzt ist, so ist

$$\frac{p-1}{4} = \frac{a^2-1}{4} + \frac{b^2}{4} \equiv \frac{b^2}{4}, \quad \frac{p_1-1}{4} = \frac{\alpha^2-1}{4} + \frac{\beta^2}{4} \equiv \frac{\beta^2}{4}$$

und folglich $\frac{p-1}{4} \cdot \frac{p_1-1}{4} \equiv \left(\frac{b\beta}{4}\right)^2$ also auch $\equiv \frac{b\beta}{4} \pmod{2}$. Die Formel (21) kann daher auch so geschrieben werden:

$$\left(\left(\frac{a+bi}{\alpha+\beta i}\right)\right) = (-1)^{\frac{p-1}{4} \cdot \frac{p_1-1}{4}} \cdot \left(\left(\frac{\alpha+\beta i}{a+bi}\right)\right).$$

Da $\frac{q^2-1}{4}$ eine gerade Zahl ist, ebenso wie $\frac{q_1^2-1}{4}$, so kann man den Formeln (17) und (22) auch folgende Gestalt geben:

$$\left(\left(\frac{\varpi}{q}\right)\right) = (-1)^{\frac{q^2-1}{4}\cdot\frac{p-1}{4}}\cdot\left(\left(\frac{-q}{\varpi}\right)\right),$$

$$\left(\left(\frac{-q_1}{q}\right)\right) = (-1)^{\frac{q^2-1}{4}\cdot\frac{q_1^2-1}{4}}\cdot\left(\left(\frac{-q}{q_1}\right)\right)$$

und diese Formeln sind offenbar nebst der vorigen in der einzigen enthalten, welche folgt:

$$(23)\qquad \left(\left(\frac{m}{m'}\right)\right) = (-1)^{\frac{\mu-1}{4}\cdot\frac{\mu'-1}{4}}\cdot\left(\left(\frac{m'}{m}\right)\right),$$

und in welcher m, m' zwei primäre complexe Primzahlen, μ, μ' ihre Normen bezeichnen. Diese Gleichung giebt das biquadratische Reciprocitätsgesetz und enthält folgenden Satz:

Die biquadratischen Charactere zweier primärer complexer Primzahlen sind einander gleich, wenn wenigstens eine der Primzahlen $\equiv 1 \pmod{4}$ ist; sie sind dagegen einander entgegengesetzt, wenn beide Primzahlen $\equiv 3+2i \pmod{4}$ sind.

In der That, in dem ersten dieser Fälle ist wenigstens eine der Normen μ, μ' von der Form $8n+1$, also einer der Factoren $\frac{\mu-1}{4}$, $\frac{\mu'-1}{4}$ gerade, während im andern Falle beide Normen von der Form $8n+5$, also beide Factoren des Exponenten von -1 ungerade sind.

Erhebt man die Gleichung (23) zum Quadrat, und beachtet, dass

$$\left(\left(\frac{-1}{m}\right)\right)^2 = \left(\left(\frac{i}{m}\right)\right)^4 = +1,\quad \left(\left(\frac{-1}{m'}\right)\right)^2 = \left(\left(\frac{i}{m'}\right)\right)^4 = +1,$$

ist, so ergiebt sich

$$(24)\qquad \left(\left(\frac{\pm m}{m'}\right)\right)^2 = \left(\left(\frac{\pm m'}{m}\right)\right)^2,$$

d. h. nach Gleichung (8) vor. Vorlesung folgendes quadratische Reciprocitätsgesetz für die complexen Zahlen von der Form $a+bi$:

Die quadratischen Charactere zweier complexer Primzahlen, deren reelle Theile ungerade sind, haben gleichen Werth.

Diese beiden Reciprocitätsgesetze sind zuerst von Gauss ausgesprochen worden,*) dagegen hat zuerst Eisenstein zwei Beweise derselben veröffentlicht,**) welche zu einander in derselben Beziehung stehen, wie die beiden in Nr. 6 und 7 der 9. Vorlesung angeführten Eisenstein'schen Beweise des quadratischen Reciprocitätsgesetzes für reelle Primzahlen. Dem ersten derselben sind wir hier gefolgt. Uebrigens gebührt Jacobi der Ruhm, schon vor Eisenstein's Publicationen in seinen Vorlesungen über Zahlentheorie einen Beweis der genannten Sätze mitgetheilt zu haben, welcher nur unwesentlich von den vorstehenden Betrachtungen verschieden ist. Ausserdem hat auch Lebesgue in seinen recherches sur les nombres***) die Theorie der biquadratischen Reste, und zwar auf derselben Grundlage behandelt, die er für die der quadratischen Reste angewendet hat.

Der Ergänzungssatz.

7. Auf ähnlichen Betrachtungen, wie der Beweis des Reciprocitätsgesetzes, beruht die Ableitung des Satzes über das Symbol $\left(\left(\frac{1+i}{m}\right)\right)$.

Nehmen wir zuerst an, m sei eine reelle Primzahl q von der Form $4n+3$. Da für eine solche $(1+i)^q \equiv 1-i \equiv -i(1+i)$, also $(1+i)^{q-1} \equiv -i \pmod{q}$ ist, so findet man

$$(1+i)^{\frac{q^2-1}{4}} \equiv (-i)^{\frac{q+1}{4}} \equiv i^{3 \cdot \frac{q+1}{4}} \equiv i^{-\frac{q+1}{4}} \pmod{q},$$

und folglich

$$\left(\left(\frac{1+i}{q}\right)\right) = i^{-\frac{q+1}{4}}. \tag{25}$$

Eine ähnliche Formel gilt, wenn m eine reelle Primzahl p von der Form $4n+1$ ist. Sind dann ϖ, ϖ' ihre primären Factoren, so folgt aus (17) der vor. Vorlesung

$$\left(\left(\frac{1+i}{\varpi'}\right)\right) = \left(\left(\frac{1-i}{\varpi}\right)\right)^3,$$

---

*) Vergl. seine Werke Bd. II, pag. 130 und 138.

**) Eisenstein, Lois de réciprocité und Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste, in Crelle's J., Bd. 28.

***) In Liouville's Journal, Bd. 4.

also da $(1-i) = -i(1+i)$ ist,

$$\left(\left(\frac{1+i}{\varpi}\right)\right) \cdot \left(\left(\frac{1+i}{\varpi'}\right)\right) = \left(\left(\frac{1+i}{\varpi}\right)\right)^{1} \cdot \left(\left(\frac{i}{\varpi}\right)\right).$$

folglich, wegen der Gleichung $\left(\left(\frac{i}{\varpi}\right)\right) = i^{\frac{p-1}{4}}$ und nach (14) der vor. Vorlesung

$$\left(\left(\frac{1+i}{p}\right)\right) = i^{\frac{p-1}{4}}. \tag{26}$$

Nun sei m eine reelle Zahl von der Form $4n+1$, welche, in reelle Primfactoren zerlegt, durch

$$m = \Pi(-q) \,.\, \Pi(p)$$

ausgedrückt werden kann, so lässt sich zunächst leicht übersehen, dass, wenn man dieser Gleichung die Form

$$m = \Pi\left(1 - 4 \,.\, \frac{q+1}{4}\right) . \,\Pi\left(1 + 4 \,.\, \frac{p-1}{4}\right)$$

giebt, in welcher $\frac{q+1}{4}$, $\frac{p-1}{4}$ nach der Bedeutung der Zahlen p, q ganze Zahlen sein werden, das entwickelte Product die Form

$$m = 1 + 4 \,.\, \sum \frac{p-1}{4} - 4 \,.\, \sum \frac{q+1}{4} + 16z$$

haben wird, während z eine ganze Zahl bezeichnet, und die Summenzeichen dieselbe Ausdehnung haben, wie die Zeichen Π in dem Ausdrucke für m. Also wird

$$\frac{m-1}{4} \equiv \sum \frac{p-1}{4} - \sum \frac{q+1}{4} \pmod{4}.$$

Da nun nach den Formeln (25) und (26)

$$\left(\left(\frac{1+i}{m}\right)\right) = \prod \left(\left(\frac{1+i}{q}\right)\right) \cdot \prod \left(\left(\frac{1+i}{p}\right)\right) = i^{\Sigma\frac{p-1}{4} - \Sigma\frac{q+1}{4}}$$

gefunden wird, so kann man auch, sobald m eine reelle Zahl von der Form $4n+1$ bedeutet, schreiben:

$$\left(\left(\frac{1+i}{m}\right)\right) = i^{\frac{m-1}{4}} \tag{27}$$

Nach diesen Vorbemerkungen gehen wir nun, indem $\varpi = \alpha + \beta i$ eine primäre Primzahl bedeuten soll, zur Bestimmung des Symboles $\left(\left(\frac{1+i}{\varpi}\right)\right)$ von der identischen Gleichung

$$(28)\qquad \alpha(1+i) = \alpha+\beta+i(\alpha+\beta i)$$

aus. Dieselbe liefert einerseits, da α und $1+i$, folglich auch $\alpha+\beta$ durch $\alpha+\beta i$ nicht theilbar sind,

$$\left(\left(\frac{\alpha}{\alpha+\beta i}\right)\right)\cdot\left(\left(\frac{1+i}{\alpha+\beta i}\right)\right) = \left(\left(\frac{\alpha+\beta}{\alpha+\beta i}\right)\right),$$

folglich

$$(29)\qquad \left(\left(\frac{1+i}{\alpha+\beta i}\right)\right) = \left(\left(\frac{\alpha}{\alpha+\beta i}\right)\right)^3\cdot\left(\left(\frac{\alpha+\beta}{\alpha+\beta i}\right)\right).$$

Andererseits folgt aus (28) auch, da $\alpha+\beta$ ungerade, also zu $1+i$ sowohl wie natürlich auch zu α relative Primzahl ist, Letzteres, weil in der complexen Primzahl ϖ α mit β keinen gemeinsamen Theiler haben kann,

$$\left(\left(\frac{\alpha+\beta i}{\alpha+\beta}\right)\right) = \left(\left(\frac{\alpha}{\alpha+\beta}\right)\right)\cdot\left(\left(\frac{1+i}{\alpha+\beta}\right)\right)\cdot\left(\left(\frac{i}{\alpha+\beta}\right)\right)^3.$$

Hierfür erhält man nach den Gleichungen (18) und (20) der vorigen Vorlesung sowie nach der Gleichung (27), welche auf den Fall $m = \alpha+\beta$ anwendbar ist, da bei jeder primären Primzahl $\alpha+\beta \equiv 1 \pmod 4$ ist, den Werth:

$$\left(\left(\frac{\alpha+\beta i}{\alpha+\beta}\right)\right) = i^{\frac{\alpha+\beta-1}{4}+3.\frac{(\alpha+\beta)^2-1}{4}}.$$

Dieser Werth kann noch einfacher ausgedrückt werden, wenn man beachtet, dass für eine Zahl m von der Form $4n+1$

$$\frac{m^2-1}{4} = 4n^2+2n\,,\quad\text{also}\quad \frac{m^2-1}{4} \equiv 2n \equiv \frac{m-1}{2} \pmod 4$$

ist; daher kann der Exponent von i gleich

$$\frac{\alpha+\beta-1}{4}+3.\frac{\alpha+\beta-1}{2}$$

geschrieben werden und ist (mod. 4) der Zahl $3\,.\,\frac{\alpha+\beta-1}{4}$ congruent, da $\alpha+\beta-1$ durch 4 theilbar ist. Da endlich das Symbol $\left(\left(\frac{\alpha+\beta}{\alpha+\beta i}\right)\right)$ nach Nr. 5 umgekehrt werden darf, ergiebt sich der Werth des zweiten Factors in (29)

$$(30)\qquad \left(\left(\frac{\alpha+\beta}{\alpha+\beta i}\right)\right) = i^{3/4(\alpha+\beta-1)}.$$

Um auch den des ersten zu bestimmen, unterscheiden wir die beiden Fälle, welche die primären Primzahlen darbieten können. Ist erstens $\alpha \equiv 1 \pmod 4$, also β durch 4 theilbar, so

kann nach Nr. 5 das Symbol $\left(\left(\frac{\alpha}{\alpha+\beta i}\right)\right)$ in

$$\left(\left(\frac{\alpha+\beta i}{\alpha}\right)\right)=\left(\left(\frac{\beta}{\alpha}\right)\right)\cdot\left(\left(\frac{i}{\alpha}\right)\right)=i^{\frac{\alpha^2-1}{4}}$$

vertauscht werden, was man nach dem soeben Gesagten auch einfacher gleich $i^{\frac{\alpha-1}{2}}$ schreiben darf. Dann wird nach (29) und (30)

$$\left(\left(\frac{1+i}{\alpha+\beta i}\right)\right)=i^{{}^3/_4(\alpha+\beta-1)+3.\frac{\alpha-1}{2}}.$$

Der Exponent von i ist gleich $\frac{\alpha-\beta-1}{4}+(\alpha+\beta-1)+(\alpha-1)$; da β durch 4 theilbar, so ist es $\frac{\beta^2}{4}$ ebenfalls, dieser Ausdruck ist daher dem folgenden: ${}^1/_4\,(\alpha-\beta-\beta^2-1)$ (mod. 4) congruent, und man findet endlich:

$$\left(\left(\frac{1+i}{\alpha+\beta i}\right)\right)=i^{{}^1/_4(\alpha-\beta-\beta^2-1)}. \tag{31}$$

Ist zweitens $\alpha\equiv-1$ (mod. 4), also $\beta\equiv2$, so kann man

$$\left(\left(\frac{\alpha}{\alpha+\beta i}\right)\right)=\left(\left(\frac{-\alpha}{\alpha+\beta i}\right)\right)\cdot\left(\left(\frac{-1}{\alpha+\beta i}\right)\right)$$

setzen, worin für den zweiten Factor sich der Werth $(-1)^{\frac{p-1}{4}}$, also, da p hier die Form $8n+5$ haben muss (siehe Nr. 3), der Werth -1 ergiebt, während der erste nach Nr. 5 umgekehrt und gleich

$$\left(\left(\frac{\alpha+\beta i}{\alpha}\right)\right)=\left(\left(\frac{\beta}{\alpha}\right)\right)\cdot\left(\left(\frac{i}{\alpha}\right)\right)=i^{\frac{\alpha^2-1}{4}}$$

gesetzt werden kann. Da hier α von der Form $4n-1$ ist, findet man

$$\frac{\alpha^2-1}{4}=4n^2-2n\equiv\frac{\alpha+1}{2}\ (\text{mod. }4),$$

also liefern die Gleichungen (29) und (30) in diesem Falle die Formel:

$$\left(\left(\frac{1+i}{\alpha+\beta i}\right)\right)=-i^{{}^3/_4(\alpha+\beta-1)+3.\frac{\alpha+1}{2}}=i^{{}^3/_4(\alpha+\beta-1)+3\frac{\alpha+1}{2}+2}.$$

Der Exponent von i kann folgendermassen geschrieben werden:

$$\tfrac{1}{4}(\alpha-\beta-5)+4+(\alpha+\beta-1)+(\alpha+1),$$

ist also (mod. 4) der Zahl ${}^1/_4\,(\alpha-\beta-5)$ oder, da hier β von

der Form $4n + 2$, also $\beta^2 \equiv 4 \pmod{16}$ und $\frac{\beta^2}{4} \equiv 1 \pmod{4}$ ist, der Zahl $\frac{1}{4}(\alpha - \beta - \beta^2 - 1)$ congruent, und so erhält man auch für diesen Fall die Gleichung (31).

Beachtet man nun, dass eine primäre Primzahl $-q$ aus der Formel $\alpha + \beta i$ hervorgeht, wenn $\alpha = -q$, $\beta = 0$ gesetzt wird, so lassen sich die, durch die Formeln (25) und (31) ausgedrückten Resultate in den allgemeinen Satz zusammenfassen:

Bedeutet $\alpha + \beta i$ eine primäre (eingliedrige oder zweigliedrige) complexe Primzahl, so ist

$$(32) \qquad \left(\left(\frac{1+i}{\alpha + \beta i}\right)\right) = i^{\frac{1}{4}(\alpha - \beta - \beta^2 - 1)} .$$

Auch dieser Satz, von welchem wir den Eisenstein'schen Beweis hier mitgetheilt haben, findet sich bereits in der 2ten Abhandlung über biquadratische Reste in Gauss' Werken Bd. II pag. 135.

Vierzehnte Vorlesung.

Die complexen Zahlen $a + b\varrho$. Das Reciprocitätsgesetz für die cubischen Reste.

1. Eine gegen p prime Zahl m wird cubischer Rest oder Nichtrest von p genannt, jenachdem die Congruenz $x^3 \equiv m \pmod{p}$ eine Lösung gestattet oder nicht. Wie es nun bei den biquadratischen Resten durchaus nothwendig war, zur Ergründung ihrer Theorie das Gebiet der reellen Zahlen zu erweitern und die complexen Zahlen von der Form $a + bi$ in Betrachtung zu ziehen, so muss man ähnlicherweise die Theorie der cubischen Reste auf die Betrachtung der complexen Zahlen von der Form $a + b\varrho$ gründen, in welchen ϱ eine imaginäre Cubikwurzel der Einheit, nämlich $\varrho = \frac{-1 + \sqrt{-3}}{2}$ ist. Bevor wir daher die Gesetze, welche die Lehre von den cubischen Resten ausmachen, hier ableiten können, müssen wir wieder die Eigenschaften jener complexen Zahlen auseinandersetzen. Da jedoch hier Alles sich sehr ähnlich verhält, wie bei

den complexen Zahlen $a + bi$, so werden wir nur Dasjenige ausführlich behandeln, was abweichend ist, alles Andere dagegen nur andeuten. —

Zu jeder Zahl $a + b\varrho$ gehört die sogenannte **conjugirte Zahl** $a + b\varrho^2$, welche statt ϱ die andere imaginäre Cubikwurzel der Einheit $\varrho^2 = \frac{-1-\sqrt{-3}}{2}$ enthält, und mit Hilfe der Gleichung $1 + \varrho + \varrho^2 = 0$ auf die Form $(a - b) - b\varrho$ gebracht werden kann. Das Product der beiden conjugirten Zahlen

$$(a + b\varrho)(a + b\varrho^2) = a^2 - ab + b^2$$

heisst ihre **Norm**, in Zeichen: $N(a + b\varrho)$.

Jede Zahl, deren Norm die Einheit ist, wird eine complexe Einheit genannt. Aus der ersten der beiden Gleichungen

$$(a + b)^2 - 3ab = 1, \quad (a - b)^2 + ab = 1,$$

welche mit der Gleichung $a^2 - ab + b^2 = 1$ identisch sind, ergiebt sich, dass a, b gleiches Zeichen haben müssen, wenn sie nicht Null sind; es ergeben sich also die Lösungen: $a = 0, b = \pm 1$; $a = \pm 1$, $b = 0$ und aus der zweiten jener Gleichungen: $a - b = 0$ also $a = b$, und $a^2 = 1$, d. h. noch zwei andere Lösungen: $a = 1$, $b = 1$; $a = -1$, $b = -1$. Hiernach existiren nur folgende sechs Einheiten:

$$+1, -1, +\varrho, -\varrho, 1 + \varrho = -\varrho^2, -1 - \varrho = +\varrho^2.$$

Die Zahl 3 ist in der Theorie der complexen Zahlen $a + b\varrho$ keine Primzahl, vielmehr das Product der beiden conjugirten Factoren $1 - \varrho$ und $1 - \varrho^2$. Der zweite derselben kann auch gleich $-\varrho^2(1 - \varrho)$ gesetzt werden, ist also nur unwesentlich vom ersten verschieden.

Jenachdem die Norm einer complexen Zahl $a + b\varrho$ durch 3 theilbar oder nicht theilbar ist, hat $a + b\varrho$ den Factor $1 - \varrho$ oder nicht. Denn, ist

$$a + b\varrho = (1 - \varrho)(\alpha + \beta\varrho),$$

so ist offenbar $N(a + b\varrho)$ durch $N(1 - \varrho) = 3$ theilbar; aber auch umgekehrt, wenn $a^2 - ab + b^2 = (a + b)^2 - 3ab$ durch 3 theilbar ist, so ergiebt sich $a + b \equiv 0$, $b \equiv -a$ (mod. 3) d. h. $b = 3m - a$, also

$$a + b\varrho = 3m\varrho + a(1 - \varrho).$$

Es bezeichne nun $a + b\varrho$ eine nicht durch $1 - \varrho$ theilbare

Zahl, so erhält man durch Multiplication mit den sechs Einheiten folgende Gruppe von associirten Zahlen:

$$\pm (a + b\varrho), \quad \pm (b + (b - a)\varrho), \quad \pm (b - a - a\varrho).$$

Da $a + b\varrho$ durch $1 - \varrho$ nicht theilbar ist, hat $N(a + b\varrho)$ die Form $3n + 1$ oder $3n - 1$, demnach folgt aus der Congruenz $a^2 - ab + b^2 \equiv (a + b)^2$ (mod. 3) die andere: $a + b \equiv \pm 1$ (mod. 3), d. h. entweder: $a \equiv \pm 1$, $b \equiv 0$, oder $a \equiv \pm 1$, $b \equiv \pm 1$ also $b - a \equiv 0$, oder: $a \equiv 0$, $b \equiv \pm 1$ also $b - a \equiv \pm 1$ (mod. 3). Diese Betrachtung zeigt, dass unter den sechs associirten Zahlen stets eine einzige existirt, welche der Bedingung Genüge leistet, dass der Coëfficient von ϱ durch 3 theilbar, der andere Theil $\equiv -1$ (mod. 3) ist. Diese Zahl soll die primäre Zahl der Gruppe genannt werden.

Jede Zahl $a + b\varrho$ kann dadurch, dass man dem ϱ seinen Werth substituirt, auf die Form $\frac{A + B\sqrt{-3}}{2}$ gebracht werden, worin

$$A = 2a - b, \quad B = b, \text{ also } A \equiv B \text{ (mod. 2)}$$

ist. Umgekehrt ist $\frac{A + B\sqrt{-3}}{2}$ stets einer complexen Zahl $a + b\varrho$ gleich, wenn $A \equiv B$ (mod. 2) ist, denn man braucht nur zu setzen:

$$b = B, \; a = \frac{A + B}{2}.$$

2. Die reellen Primzahlen, mit Ausnahme der Drei, zerfallen in zwei Gruppen: in Primzahlen von der Form $6n + 5$ und solche von der Form $6n + 1$. Die erstern spielen auch in der Theorie der complexen Zahlen $a + b\varrho$ die Rolle von Primfactoren, d. h. sie sind nicht weiter in Factoren zerlegbar, welche von Einheiten verschieden sind. Wäre nämlich eine solche Primzahl q dem Producte zweier complexer Factoren gleich, etwa

$$q = \frac{A + B\sqrt{-3}}{2} \cdot \frac{A' + B'\sqrt{-3}}{2},$$

so ergäbe sich daraus

$$q^2 = \frac{A^2 + 3B^2}{4} \cdot \frac{A'^2 + 3B'^2}{4},$$

worin die beiden Factoren als Normen complexer Zahlen ganze reelle Zahlen sein müssen. Eine derselben muss durch q theilbar sein, z. B.

$$A^2 + 3B^2 \equiv 0 \text{ (mod. } q);$$

entweder folgen hieraus $A = \alpha q$, $B = \beta q$, während α, β ganzzahlig sind; da aber dann

$$1 = \frac{\alpha^2 + 3\beta^2}{4} \cdot \frac{A'^2 + 3B'^2}{4}$$

wäre, so würden die complexen Zahlen $\frac{\alpha + \beta\sqrt{-3}}{2}$, $\frac{A' + B'\sqrt{-3}}{2}$ Einheiten sein, was keine eigentliche Zerlegung von q ergäbe. Oder man findet A, B nicht durch q theilbar, wo dann eine Zahl β der Congruenz $B\beta \equiv 1 \pmod{q}$ gemäss bestimmt werden kann, und sich $(A\beta)^2 \equiv -3 \pmod{q}$ d. h.

$$\left(\frac{-3}{q}\right) = +1,$$

nach dem quadratischen Reciprocitätsgesetz und Gl. (7) Vorl. 9 also auch

$$\left(\frac{q}{3}\right) = \left(\frac{2}{3}\right) = +1$$

ergiebt, während doch unter den beiden Resten 1, 2 (mod. 3) der erstere den quadratischen Rest, also der letztere den quadratischen Nichtrest von 3 repräsentirt.

Wenn so die reellen Primzahlen der Form $6n + 5$ auch als complexe Zahlen Primzahlen bleiben, weiss man aus Nr. 1 der 11. Vorlesung, dass jede Primzahl von der Form $6n + 1$ in zwei conjugirte complexe Factoren zerlegbar ist, von denen man sich, wie in Nr. 3 der 12. Vorlesung bezüglich der complexen Factoren der reellen Primzahlen $4n + 1$, leicht überzeugt, dass sie nun die Rolle von Primfactoren übernehmen.

Es giebt demnach hier drei verschiedene Arten von Primfactoren: die Zahl $1 - \varrho$, die reellen Primzahlen der Form $6n + 5$, und die zweigliedrigen Primzahlen, welche reelle Primzahlen der Form $6n + 1$ zu Normen haben. Die zweite Gattung ist primär, die Zahl $1 - \varrho$ soll als primäre ihrer Gruppe bezeichnet werden, die Zahlen der dritten Gattung werden es, mit einer passenden Einheit multiplicirt. Genau auf demselben Wege, wie bei den complexen Zahlen $a + bi$, lässt sich beweisen, dass jede complexe Zahl nur auf eine einzige Weise als Product solcher primärer Primzahlen dargestellt werden kann.

3. Dazu genügt es nach der allgemeinen Bemerkung in Nr. 4 der 12. Vorlesung, Zweierlei nachzuweisen: Erstens, dass ein endlicher Algorithmus

zur Berechnung des grössten gemeinsamen Theilers zweier complexer Zahlen existirt, was durch folgenden Satz (nach der eben angeführten Nummer) offenbar erreichbar wird:

Sind $m = \frac{A + B\sqrt{-3}}{2}$ und $m' = \frac{A' + B'\sqrt{-3}}{2}$ zwei complexe Zahlen von der Art $a + b\varrho$, so giebt es stets eine complexe Zahl $z = \frac{x + y\sqrt{-3}}{2}$ derselben Art, von der Beschaffenheit, dass $N(m - m'z) < \frac{1}{2} N(m')$ ist. Denn, setzt man

$$2 \cdot \frac{A + B\sqrt{-3}}{A' + B'\sqrt{-3}} = \alpha + \beta\sqrt{-3},$$

sodass

$$\alpha = 2 \cdot \frac{A A' + 3 B B'}{A'^2 + 3 B'^2}, \quad \beta = 2 \cdot \frac{B A' - A B'}{A'^2 + 3 B'^2}$$

ist, und wählt für y diejenige ganze Zahl, welche β am Nächsten liegt, für x dagegen diejenige der beiden, α umgebenden, Zahlen, welche mit y gleichartig ist, so ist $\frac{x + y\sqrt{-3}}{2}$ eine complexe, aus ϱ gebildete, Zahl von der Beschaffenheit, dass

$$(N(\alpha - x) + (\beta - y)\sqrt{-3}) \text{ d.h. } N\left(2 \cdot \frac{A + B\sqrt{-3}}{A' + B'\sqrt{-3}} - (x + y\sqrt{-3})\right) < 2,$$

also

$$N\left(\frac{A + B\sqrt{-3}}{2} - \frac{A' + B'\sqrt{-3}}{2} \cdot \frac{x + y\sqrt{-3}}{2}\right) < \frac{1}{2} \cdot N\left(\frac{A' + B'\sqrt{-3}}{2}\right)$$

ist, was zu zeigen war.

Zweitens muss gezeigt werden, dass ausser den oben bezeichneten Primzahlen keine andern existiren, was ganz ähnlich geschieht, wie in der vorletzten Vorlesung. —

Definirt man nun wieder zwei complexe Zahlen n, n' als congruent (mod. m), wenn ihre Differenz durch die (complexe) Zahl m theilbar ist, so gelten die gewöhnlichen Regeln und Sätze, darunter namentlich der Satz, dass eine Congruenz, welche in Bezug auf einen Primzahlmodulus stattfindet, nie mehr incongruente Wurzeln haben kann, als ihr Grad beträgt.

Sei $a + b\varrho$ eine complexe Zahl, so werden alle diejenigen complexen Zahlen, welche mod. $(a + b\varrho)$ der Zahl $\alpha + \beta\varrho$ congruent sind, durch die Gleichung

$$x + y\varrho = (a + b\varrho)(t + u\varrho) + \alpha + \beta\varrho$$

bestimmt, wenn t, u alle möglichen ganzzahligen Werthe erhalten. Aus dieser Gleichung ergeben sich aber

$$x = at - bu + \alpha, \quad y = bt + (a - b)u + \beta .$$

Ist also d grösster gemeinsamer Theiler von a und b, also auch von $a - b$ und b, so muss $y \equiv \beta$ (mod. d) sein, und, wenn y_0 der kleinste Werth ist, welcher dieser Bedingung genügt, so hat die Gleichung

$$bt + (a - b)u = y_0 - \beta$$

unendlich viel ganzzahlige Lösungen der Art, dass die Formeln

$$t = t_0 + \frac{a - b}{d} \cdot z, \quad u = u_0 - \frac{b}{d} z$$

alle Lösungen ergeben, wenn t_0, u_0 eine derselben, und z eine unbestimmte ganze Zahl bezeichnet. Dann findet man aber

$$x = at_0 - bu_0 + \alpha + \frac{a^2 - ab + b^2}{d} \cdot z,$$

und es giebt einen bestimmten Werth des z, für welchen x kleiner wird als $\frac{a^2 - ab + b^2}{d}$. Der entsprechende Werth von x heisse x_0, dann ist

$$x_0 + y_0\varrho \equiv \alpha + \beta\varrho \text{ mod. } (a + b\varrho)$$

und der Beweis geliefert, dass unter allen Zahlen $x + y\varrho$, bei welchen x, y die Werthe aus den beiden Reihen:

$$0, 1, 2, \ldots \left(\frac{a^2 - ab + b^2}{d} - 1\right); \quad 0, 1, 2, \ldots (d - 1)$$

resp. erhalten, stets eine einzige einer gegebenen Zahl mod. $(a + b\varrho)$ congruent ist, mit andern Worten: es giebt $a^2 - ab + b^2$ incongruente Reste, und die Zahlen $x + y\varrho$ constituiren ein vollständiges Restensystem mod. $(a + b\varrho)$. —

4. Ist nun $m = a + b\varrho$ eine von $1 - \varrho$ verschiedene Primzahl, so ergiebt sich wieder sehr leicht das Analogon des Fermat'schen Lehrsatzes: Für jede, durch m nicht theilbare, complexe Zahl n besteht die Congruenz

$$n^{\mu - 1} \equiv 1 \text{ (mod. } m), \tag{1}$$

in welcher μ die Norm von m bedeutet. Diese Norm ist gleich q^2, wenn m eine reelle Primzahl q von der Form $6n + 5$ bezeichnet, dagegen gleich p, wenn m ein Factor einer reellen

Primzahl p von der Form $6n+1$ ist; in allen Fällen also ist μ von der Form $6n+1$.

Aus dieser Bemerkung folgt, dass die Congruenz (1) auch folgende Darstellung zulässt:

$$(n^{\frac{\mu-1}{3}}-1)(n^{\frac{\mu-1}{3}}-\varrho)(n^{\frac{\mu-1}{3}}-\varrho^2)\equiv 0 \pmod{m}\,.$$

Alle, durch m nicht theilbaren, Reste zerfallen demnach in drei Classen von je $\frac{\mu-1}{3}$ Zahlen, welche resp. die Wurzeln der drei Congruenzen

$$(2)\qquad n^{\frac{\mu-1}{3}}\equiv 1,\ n^{\frac{\mu-1}{3}}\equiv \varrho,\ n^{\frac{\mu-1}{3}}\equiv \varrho^2 \pmod{m}$$

sind.

Die Zahlen der ersten Classe sind die cubischen Reste von m. Zum Beweise dieses Hauptsatzes gelangt man mittelst derselben Betrachtungen, wie in Nr. 7 der vorletzten Vorlesung, nur dass hier ein anders zusammengesetztes Restsystem (mod. m) zu Grunde gelegt werden muss, dessen Existenz leicht zu erkennen ist, nämlich ein, aus drei solchen Gruppen von $\frac{\mu-1}{3}$ Gliedern bestehendes Restsystem, dass, wenn r die Zahlen der einen Gruppe bezeichnet, die der beiden andern durch $r\varrho$ und $r\varrho^2$ resp. ausgedrückt werden.

Unter dem cubischen Character einer durch m nicht theilbaren Zahl n soll hinfort diejenige Potenz von ϱ verstanden werden, welche in der Congruenz

$$n^{\frac{\mu-1}{3}}\equiv \varrho^{\bullet} \pmod{m}$$

gewählt werden muss. Führen wir für denselben das von Eisenstein benutzte Zeichen $\left[\frac{n}{m}\right]$ ein, so ergiebt sich demnach die Congruenz

$$(3)\qquad n^{\frac{\mu-1}{3}}\equiv\left[\frac{n}{m}\right] \pmod{m}.$$

Auch hier sei, wenigstens in aller Kürze, des Analogons des Gauss'schen Lemma gedacht, dessen Beweis, auf dem vorher angegebenen Restsysteme beruhend, nach den früheren Mittheilungen keinen Schwierigkeiten unterliegt. Dies ist folgender

Satz: Ist n eine durch m nicht theilbare Zahl, und werden α, β, γ von den $\frac{\mu-1}{3}$ Zahlen $n \,.\, r$ resp. Zahlen der Gruppen $r, r\varrho, r\varrho^2$ resp. (mod. m) congruent, so ist

$$(4) \qquad \left[\frac{n}{m}\right] = \varrho^{\beta+2\gamma}.$$

5. Da auch das Symbol für den cubischen Character offenbar ausser der Gleichung

$$(5) \qquad \left[\frac{n'}{m}\right] = \left[\frac{n}{m}\right], \text{ wenn } n' \equiv n \text{ (mod. } m) \text{ ist,}$$

auch der andern Gleichung

$$(6) \qquad \left[\frac{n n'}{m}\right] = \left[\frac{n}{m}\right] \cdot \left[\frac{n'}{m}\right],$$

in welcher n, n' zwei gleiche oder verschiedene, durch m nicht theilbare Zahlen bedeuten, Genüge leistet, der cubische Character eines Products also durch die seiner Factoren bestimmt wird, so genügt es, im Folgenden die einfachen Fälle zu betrachten:

$$n = -1, \; n = \varrho, \; n = 1 - \varrho, \; n = m',$$

wo m' eine von m verschiedene complexe Primzahl bedeutet, und die Werthe der zugehörigen Symbole

$$\left[\frac{-1}{m}\right], \; \left[\frac{\varrho}{m}\right], \; \left[\frac{1-\varrho}{m}\right], \; \left[\frac{m'}{m}\right]$$

zu bestimmen. Für das letzte existirt wieder ein sehr einfaches Reciprocitätsgesetz, das dritte soll später untersucht, die ersten beiden aber können unmittelbar gefunden werden.

Ist nämlich n eine reelle Zahl und q eine reelle Primzahl von der Form $6m + 5$, sodass $\frac{q+1}{3}$ eine ganze Zahl ist, so folgt aus dem Fermat'schen Satze: $n^{q-1} \equiv 1$ (mod. q) die Congruenz

$$(n^{q-1})^{\frac{q+1}{3}} = n^{\frac{q^2-1}{3}} \equiv 1 \quad \text{(mod. } q)$$

und folglich

$$(7) \qquad \left[\frac{n}{q}\right] = +1.$$

Hiernach ist z. B. $\left[\frac{-1}{q}\right] = +1$. Ebenso aber ist, wenn $a + b\varrho$ Factor einer Primzahl p von der Form $6n + 1$ ist, nach der Definition

$$\left[\frac{-1}{a+b\varrho}\right]=(-1)^{\frac{p-1}{3}}=+1,$$

also findet man allgemein:

$$(8)\qquad \left[\frac{-1}{m}\right]=+1.$$

Aus der Definition des Symbols selbst ergiebt sich ferner sofort die Congruenz

$$\left[\frac{\varrho}{m}\right]\equiv\varrho^{\frac{\mu-1}{3}}\quad(\text{mod. } m),$$

oder, weil m von $1-\varrho$ verschieden vorausgesetzt ist, die Gleichung:

$$(9)\qquad \left[\frac{\varrho}{m}\right]=\varrho^{\frac{\mu-1}{3}}.$$

Schliesslich sei hier eine einfache Bemerkung angefügt. Ist $\varrho^{\mathfrak{s}}$ der Werth des Symboles $\left[\frac{\alpha+\beta\varrho}{a+b\varrho}\right]$, so besteht die Congruenz:

$$(\alpha+\beta\varrho)^{\frac{\mu-1}{3}}\equiv\varrho^{\mathfrak{s}}\quad(\text{mod. } a+b\varrho),$$

d. h. eine Gleichung von der Form

$$(\alpha+\beta\varrho)^{\frac{\mu-1}{3}}=\varrho^{\mathfrak{s}}+(a+b\varrho)(A+B\varrho),$$

in welcher $\mu=N(a+b\varrho)$, A, B ganze reelle Zahlen sind, und welche wegen der Irreductibilität der Gleichung $\varrho^2+\varrho+1=0$ auch bestehen muss, wenn ϱ^2 statt ϱ gesetzt wird; dadurch aber ergiebt sich

$$(\alpha+\beta\varrho^2)^{\frac{\mu-1}{3}}=\varrho^{2\mathfrak{s}}+(a+b\varrho^2)(A+B\varrho^2)$$

oder

$$(\alpha+\beta\varrho^2)^{\frac{\mu-1}{3}}\equiv\varrho^{2\mathfrak{s}}\quad(\text{mod. } a+b\varrho^2),$$

d. h. der Werth des Symbols $\left[\frac{\alpha+\beta\varrho^2}{a+b\varrho^2}\right]$ ist $\varrho^{2\mathfrak{s}}$. Aus dieser Bemerkung erhält man die nützliche Gleichung:

$$(10)\qquad \left[\frac{\alpha+\beta\varrho^2}{a+b\varrho^2}\right]=\left[\frac{\alpha+\beta\varrho}{a+b\varrho}\right]^2.$$

Beweis des Reciprocitätsgesetzes.

6. Nachdem im Vorigen die arithmetische Grundlage für die Theorie der cubischen Reste gelegt worden, müssen nun die-

jenigen Formeln aus der Kreistheilung zusammengestellt werden, durch deren Hilfe der Beweis des Reciprocitätsgesetzes sich ergiebt. Wir sind darauf bereits in Nr. 2 der 11. Vorlesung geführt worden. Bezeichnen wir hinfort mit T_1, T_2 die beiden Ausdrücke:

$$(\varrho, r) = \sum_{\mu=1}^{\mu=p-1} \varrho^{\text{ind}.\mu} \cdot r^{\mu}, \quad (\varrho^2, r) = \sum_{\mu=1}^{\mu=p-1} \varrho^{2\,\text{ind}.\mu} \cdot r^{\mu},$$

so liefern die Formeln der angeführten Nr. folgende Gleichungen:

$$(11) \qquad T_1 \cdot T_2 = (-1)^{\frac{p-1}{3}} \cdot p,$$

$$(12) \qquad T_1^3 = p(a + b\varrho), \quad T_2^3 = p(a + b\varrho^2),$$

worin

$$(13) \qquad a + b\varrho = \sum_{\mu=1}^{\mu=p-2} \varrho^{\text{ind}.\mu + \text{ind}.(1+\mu)}$$

gesetzt ist. Aus den Gleichungen (12) erhält man die Ausdrücke T_1, T_2 durch Wurzelausziehung, aber mit der Unbestimmtheit behaftet, dass man nicht weiss, welche der Cubikwurzeln ihnen gleichzusetzen sind; diese Frage, welche der in Nr. 3 der 9. Vorlesung bezüglich der Summe S aufgeworfenen analog ist, ist auch hier bisher noch nicht beantwortet worden, jedoch bedarf es auch wieder ihrer Lösung nicht zum Beweise des cubischen Reciprocitätsgesetzes. Wohl aber haben wir festzustellen, ob in der durch die Kreistheilung erhaltenen Zerfällung von p in die beiden conjugirt-complexen Factoren $a + b\varrho$, $a + b\varrho^2$ diese primär sind, oder nicht. Die Antwort hierauf wird ebenfalls durch die Resultate der angeführten Nr. gegeben und fällt zu Gunsten der erstern Alternative aus, da wir dort gesehen haben, dass $a \equiv -1$, $b \equiv 0 \pmod{3}$ ist.

Bezeichnen wir also fortan mit ϖ, ϖ' die beiden conjugirt-complexen primären Factoren, in welche p zerlegbar ist, so muss ϖ mit einer dieser beiden Zahlen:

$$a + b\varrho = \frac{A + B\sqrt{-3}}{2}, \quad a + b\varrho^2 = \frac{A - B\sqrt{-3}}{2}$$

übereinstimmen. Da das Vorzeichen von B mit der willkürlichen Wahl der primitiven Wurzel g sich ändert, dürfen wir letztere so gewählt denken, dass $\varpi = a + b\varrho$ wird. Aus den beiden Congruenzen

$$a + bg^{\frac{p-1}{3}} \equiv 0, \quad a + b\varrho \equiv 0 \pmod{\varpi},$$

deren erste eine Folge der Congruenz (13) in der angeführten Vorlesung ist, schliesst man sodann, dass

$$g^{\frac{p-1}{3}} \equiv \varrho \pmod{\varpi},$$

also $\left[\frac{g}{\varpi}\right] = \varrho$ ist. Hierdurch erhalten die beiden Ausdrücke T_1, T_2 folgende Gestalt:

$$T_1 = \sum_{\mu=1}^{\mu=p-1} \varrho^{\text{ind.}\mu} \cdot r^\mu = \sum_{m=0}^{m=p-2} \varrho^m \cdot r^{g^m} = \sum_{m=0}^{m=p-2} \left[\frac{g^m}{\varpi}\right] \cdot r^{g^m}$$

oder, was dasselbe ist,

$$T_1 = \sum_{s=1}^{s=p-1} \left[\frac{s}{\varpi}\right] \cdot r^s.$$

Ebenso kommt

$$T_2 = \sum_{s=1}^{s=p-1} \left[\frac{s}{\varpi}\right]^2 \cdot r^s.$$

Ersetzt man in diesen Ausdrücken r durch r^k, während k durch p nicht theilbar ist, und bezeichnet die so entstehenden Ausdrücke mit $T_1^{(k)}$, $T_2^{(k)}$, so findet man leicht folgende Beziehungen:

$$(14) \qquad T_1^{(k)} = \left[\frac{k}{\varpi}\right]^2 \cdot T_1, \quad T_2^{(k)} = \left[\frac{k}{\varpi}\right] \cdot T_2.$$

7. Durch die soeben angegebenen Hilfsmittel können wir nunmehr das Reciprocitätsgesetz, welches in der Theorie der cubischen Reste herrscht und von allen analogen Gesetzen das einfachste ist, mit Leichtigkeit beweisen. Wir unterscheiden aber dabei vier Fälle.

1) Sind q, q' zwei reelle Primzahlen von der Form $6n + 5$, so folgt aus der Gleichung (7) sowohl $\left[\frac{q'}{q}\right] = 1$ als auch $\left[\frac{q}{q'}\right] = 1$, also ist stets

$$(15) \qquad \left[\frac{q}{q'}\right] = \left[\frac{q'}{q}\right].$$

2) Während q eine Primzahl der Form $6n + 5$ ist, sei p eine solche von der Form $6n + 1$ und ϖ, ϖ' ihre primären Factoren. Erhebt man den Ausdruck T_1 zur q^{ten}

Potenz, so ergiebt sich, indem alle durch q theilbaren Glieder der Entwicklung vernachlässigt werden, die Congruenz:

$$\left.\begin{array}{l} T_1{}^q \equiv \sum\limits_{s=1}^{s=p-1} \left[\frac{s}{\varpi}\right]^2 . r^{qs} \equiv T_2{}^{(q)} \\ \text{und folglich nach (14):} \\ T_1{}^q \equiv \left[\frac{q}{\varpi}\right] . T_2. \end{array}\right\} \pmod{q}$$

Multiplicirt man hierin mit T_1 und berücksichtigt die Gleichungen (11) und (12), so kommt:

$$(p\varpi)^{\frac{q+1}{3}} \equiv \left[\frac{q}{\varpi}\right] . p$$

und durch Erhebung zu der $(q - 1)^{ten}$ Potenz, wobei $p^{q-1} \equiv 1$ gesetzt werden darf,

$$(p\varpi)^{\frac{q^2-1}{3}} \equiv \left[\frac{q}{\varpi}\right] \pmod{q}.$$

Obwohl diese Congruenz keine gewöhnliche ist, darf sie doch wie eine solche aufgefasst werden, denn, als Gleichung geschrieben, hat sie die Form

$$(p\varpi)^{\frac{q^2-1}{3}} - \left[\frac{q}{\varpi}\right] = q . W,$$

worin W eine ganze Function von r mit ganzzahligen complexen Coëfficienten bezeichnet, ist also von der Art der Gleichung (10) in der 11. Vorlesung, und, da sie ebenso wie diese bestehen bleibt, indem man ϱ durch ϱ^2 ersetzt, wie sich leicht ergiebt, indem man mit dem Ausdrucke T_2 ebenso verfährt, als es mit T_1 geschehen ist, so gestattet sie analoge Consequenzen und führt zu dem Schlusse, dass die Differenz

$$(p\varpi)^{\frac{q^2-1}{3}} - \left[\frac{q}{\varpi}\right]$$

durch q theilbar, also endlich

$$\left[\frac{p\varpi}{q}\right] = \left[\frac{q}{\varpi}\right]$$

ist. Da nun

$$\left[\frac{p\varpi}{q}\right] = \left[\frac{p}{q}\right] . \left[\frac{\varpi}{q}\right]$$

ist, schliesst man nach Formel (7) die Gleichung:

$$(16)\qquad \left[\frac{\varpi}{q}\right] = \left[\frac{q}{\varpi}\right].$$

3) Nun seien p und p_1 zwei verschiedene Primzahlen der Form $6n+1$, jene habe die primären Factoren ϖ, ϖ', diese die primären Factoren ϖ_1, ϖ_1'. Erhebt man den Ausdruck T_1 zur p_1^{ten} Potenz und vernachlässigt alle durch p_1 theilbaren Glieder der Entwicklung, so findet man

$$T_1^{p_1} \equiv \sum_{s=1}^{s=p-1} \left[\frac{s}{\varpi}\right] . r^{p_1 s} \equiv T_1^{(p_1)} \quad (\text{mod. } p_1),$$

also nach (14):

$$T_1^{p_1} \equiv \left[\frac{p_1}{\varpi}\right]^2 . T_1,$$

woraus sich, indem man mit T_2 multiplicirt und die Gleichung (11) berücksichtigt, folgende Congruenz:

$$\left(T_1^{p_1-1} - \left[\frac{p_1}{\varpi}\right]^2\right) p \equiv 0$$

oder auch nach (12):

$$\left((p\varpi)^{\frac{p_1-1}{3}} - \left[\frac{p_1}{\varpi}\right]^2\right) p \equiv 0 \quad (\text{mod. } p_1)$$

ergiebt. Diese Congruenz findet zwar nicht im gewöhnlichen Sinne statt, jedoch findet hier die Bemerkung aus dem vorigen Falle wieder Anwendung und man erhält im gewöhnlichen Sinne

$$(p\varpi)^{\frac{p_1-1}{3}} \equiv \left[\frac{p_1}{\varpi}\right]^2 \quad (\text{mod. } p_1),$$

also, da ϖ_1 ein Factor von p_1 ist, auch (mod. ϖ_1), und daher die Gleichung

$$\left[\frac{p\varpi}{\varpi_1}\right] = \left[\frac{p_1}{\varpi}\right]^2.$$

Da nun auf demselben Wege

$$\left[\frac{p_1\varpi_1}{\varpi}\right] = \left[\frac{p}{\varpi_1}\right]^2$$

gefunden wird, so folgt zunächst durch Multiplication beider Gleichungen

$$\left[\frac{\varpi}{\varpi_1}\right] \cdot \left[\frac{\varpi_1}{\varpi}\right] = \left[\frac{p_1}{\varpi}\right] \cdot \left[\frac{p}{\varpi_1}\right],$$

und, wenn nun beiderseits mit $\left[\frac{\varpi_1}{\varpi}\right]^2$ multiplicirt und die zweite der vorhergehenden Gleichungen sowie der Umstand beachtet wird, dass der Cubus des Symbols für den cubischen Character der Einheit gleich wird, so ergiebt sich

$$(17) \qquad \left[\frac{\varpi}{\varpi_1}\right] = \left[\frac{\varpi_1}{\varpi}\right].$$

4) Hiermit wären alle Fälle erschöpft, welche man durch Combination der verschiedenen Arten complexer Primzahlen herstellen kann, wenn der vorige Beweis auf zwei conjugirte zweigliedrige Primzahlen Anwendung fände, was jedoch nicht der Fall ist, da man die Normen der Primzahlen p und p_1 als verschieden dabei vorauszusetzen hat.. Es seien daher endlich $a + b\varrho$ und $a + b\varrho^2$ zwei conjugirte primäre Primzahlen mit der Norm p, so findet sich aus den identischen Gleichungen

$$a + b\varrho = 2a - b - (a + b\varrho^2) = A - (a + b\varrho^2)$$
$$a + b\varrho^2 = 2a - b - (a + b\varrho) = A - (a + b\varrho)$$

und der Gleichung (5):

$$\left[\frac{a + b\varrho}{a + b\varrho^2}\right] = \left[\frac{A}{a + b\varrho^2}\right] \text{ und } \left[\frac{a + b\varrho^2}{a + b\varrho}\right] = \left[\frac{A}{a + b\varrho}\right].$$

Da aber nach der Congruenz (16) der 11. Vorlesung A cubischer Rest von p ist, so ist es auch ein solcher von jedem der beiden Factoren von p, die beiden Symbole haben daher den gemeinsamen Werth Eins, und man findet:

$$(18) \qquad \left[\frac{a + b\varrho}{a + b\varrho^2}\right] = \left[\frac{a + b\varrho^2}{a + b\varrho}\right].$$

In allen Fällen bleibt also die Beziehung zwischen den reciproken Symbolen dieselbe, und es ergiebt sich das sehr einfache Reciprocitätsgesetz: Sind m, m' zwei primäre Primzahlen von der Form $a + b\varrho$, so ist der cubische Character von m in Bezug auf m' dem cubischen Character von m' in Bezug auf m gleich.

Dieses Gesetz wurde zuerst von Jacobi in seiner Note über Kreistheilung ausgesprochen und ist auch in seinen Vorlesungen bewiesen worden. Der erste, übrigens ganz ähnliche Beweis,

welcher davon publicirt worden, ist der Eisenstein'sche in Crelle's J. Bd. 27*), welchen in den Hauptzügen wir hier wiedergegeben haben. Vgl. übrigens wieder Lebesgue's recherches sur les nombres, in Liouv. J. Bd. 4.

Fünfzehnte Vorlesung.

Die Bildung der Periodengleichungen. Zerfällung von X in Factoren. Die Ergänzungssätze.

1. In der 6. und 8. Vorlesung haben wir zwei Methoden kennen gelernt, um die Kreistheilungsgleichung aufzulösen: Die eine führte sie auf Hilfsgleichungen zurück, deren Wurzeln die zusammengehörigen Perioden von derselben Gliederzahl waren, die andere lehrte diese Hilfsgleichungen sowohl als die Kreistheilungsgleichung selbst direct auf reine Gleichungen zu reduciren. Obwohl nun vermittelst dieser letztern Methode die Perioden gefunden werden können, ohne die Gleichungen, deren Wurzeln sie sind, erst wirklich zu bilden, so ist die Bildung derselben doch sehr lehrreich und soll hier in einigen der einfachsten Fälle wirklich durchgeführt werden, weil auch hier wieder der wunderbare Zusammenhang zwischen der Kreistheilung und höheren Arithmetik zu Tage tritt. —

Sind wieder $\eta_0, \eta_1 \ldots \eta_{e-1}$ die e Perioden von f Gliedern, so besteht die Aufgabe, welche wir uns stellen, in der Bestimmung der Coëfficienten der Gleichung $F(x) = 0$, deren Wurzeln sie sind, mit andern Worten: in der Bestimmung der Werthe für die einfachsten symmetrischen Functionen:

$$\eta_0 + \eta_1 + \cdots + \eta_{e-1}$$

$$\eta_0\,\eta_1 + \eta_0\,\eta_2 + \eta_1\,\eta_2 + \cdots + \eta_{e-2}\,\eta_{e-1}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\eta_0\,\eta_1 \cdots \eta_{e-1},$$

---

*) Eisenstein, Beweis des Reciprocitätsgesetzes für die cubischen Reste in der Theorie der aus 3ten Wurzeln der Einheit zusammengesetzten complexen Zahlen.

denn diese sind bekanntlich, mit passendem Vorzeichen genommen, jenen Coëfficienten gleich. Die erste derselben ist als Summe aller Wurzeln der Kreistheilungsgleichung bekannt, nämlich:

$$(1)\qquad \eta_0 + \eta_1 + \dots + \eta_{e-1} = -1\,.$$

Um die übrigen zu bestimmen, kann man sich der Sätze in Nr. 6 und 7 der 6. Vorlesung bedienen, vortheilhafter aber sind folgende, von Kummer in Cr. J. Bd. 35 pag. 328 mitgetheilte Betrachtungen.

Das Product der beiden Perioden:

$$\eta_0 = \sum_{s=0}^{s=f-1} r^{g^{es}}, \quad \eta_k = \sum_{t=0}^{t=f-1} r^{g^{et+k}}$$

kann folgendermassen geschrieben werden:

$$\eta_0\,\eta_k = \sum_{s=0}^{s=f-1}\sum_{t=0}^{t=f-1} r^{g^{es}(1+g^{et+k})},$$

da für ein stehendes s die Zahlen $t+s$ und t gleichzeitig den Zahlen $0, 1, 2, \dots f-1$ (mod. f) congruent werden. Indem man nun zuerst die Summation nach s ausführt, muss man zwei Fälle unterscheiden: entweder wird für ein bestimmtes t:

$$(2)\qquad 1 + g^{et+k} \equiv 0 \pmod{p},$$

dann reducirt sich der entsprechende Theil der Doppelsumme auf f; oder aber man findet

$$(3)\qquad 1 + g^{et+k} \equiv g^{ez+h} \pmod{p},$$

während h eine der Zahlen $0, 1, 2, \dots e-1$ und z eine der Zahlen $0, 1, 2, \dots f-1$ bezeichnet; in diesem Falle wird der entsprechende Theil der Doppelsumme gleich

$$\sum_{s=0}^{s=f-1} r^{g^{e(s+z)+h}} = \eta_h\,.$$

Nun ist die Congruenz (2) gleichbedeutend mit der Gleichung $et + k = \frac{p-1}{2}$, denn $et+k$ kann nur einen der Werthe $0, 1, 2, \dots p-2$ haben, unter welchen der eben bezeichnete allein jener Congruenz genügt. Ist aber f gerade, so folgt aus dieser Gleichung, dass k durch e theilbar ist, welcher Bedingung unter den Werthen $0, 1, 2, \dots e-1$, die k erhalten kann, nur $k = 0$ entspricht, und dann giebt es nur den einen

Werth $t = \frac{f}{2}$, für den die Gleichung besteht. Ist dagegen f ungerade, so muss k durch $\frac{e}{2}$ theilbar, kann aber nicht Null sein, da sonst $f \cdot \frac{e}{2} \equiv 0 \pmod{e}$, also f gerade sein würde, also ergiebt sich $k = \frac{e}{2}$ und $t = \frac{f-1}{2}$. Versteht man hiernach unter $n^{(k)}$ die Einheit, wenn entweder f gerade und $k = 0$, oder f ungerade und $k = \frac{e}{2}$ ist, in allen andern Fällen aber die Null, so tritt allgemein der erste der obigen Fälle $n^{(k)}$ mal ein. Mit m_h^k möge ausserdem bezeichnet werden, für wieviel verschiedene Werthe des t der zweite Fall eintritt, sodass $m_h^k = 0$ ist, wenn einem Werthsysteme h, k kein, der Congruenz (3) genügendes Werthsystem t, z entspricht. Dann ist offenbar

$$(4) \quad \eta_0 \eta_k = n^{(k)} \cdot f + m_0^k \cdot \eta_0 + m_1^k \cdot \eta_1 + \ldots + m_{e-1}^k \cdot \eta_{e-1},$$

also, indem in dieser Gleichung r^{g^m} statt r gesetzt wird, wodurch die Perioden $\eta_0, \eta_1, \ldots \eta_{e-1}$ um m Stellen cyclisch vertauscht werden, auch

$$(5) \quad \eta_m \cdot \eta_{m+k} = n^{(k)} \cdot f + m_0^k \cdot \eta_m + m_1^k \cdot \eta_{m+1} + \ldots + m_{e-1}^k \cdot \eta_{m-1}.$$

Mit Leichtigkeit ergeben sich einige allgemeine Eigenschaften der Coëfficienten m_h^k. Da zunächst jede Periode f Glieder enthält, so hat das Product $\eta_0 \cdot \eta_k$ deren f^2, aus der Darstellung desselben in der Form (4) folgt daher unmittelbar die Gleichung

$$(6) \qquad n^{(k)} + m_0^k + m_1^k + \ldots + m_{e-1}^k = f,$$

und mit Rücksicht auf sie findet man dann

$$\eta_0\eta_k + \eta_1\eta_{k+1} + \ldots + \eta_{e-1}\eta_{k-1} = n^{(k)} \cdot ef - m_0^k - m_1^k - \ldots - m_{e-1}^k$$

$$(7) \qquad = n^{(k)} \cdot p - f,$$

also auch

$$\eta_m \cdot \eta_{k+m} + \eta_{m+1} \cdot \eta_{k+m+1} + \ldots + \eta_{m-1} \cdot \eta_{k+m-1} = n^{(k)} \cdot p - f,$$

oder, wenn k statt $k+m$ gesetzt wird:

$$(8) \quad \eta_m \eta_k + \eta_{m+1} \eta_{k+1} + \ldots + \eta_{m-1} \eta_{k-1} = n^{(k-m)} \cdot p - f.$$

Ferner wollen wir die Gleichung (4) mit η_h multipliciren und in der so gebildeten Gleichung r successive durch r^g, $r^{g^2}, \ldots r^{g^{e-1}}$ ersetzen, wodurch sich folgendes System von Gleichungen ergiebt:

$$\eta_0\eta_h\eta_k = n^{(k)}.f.\eta_h + m_0^k.\eta_0\eta_h + m_1^k.\eta_1\eta_h + \ldots + m_{e-1}^k.\eta_{e-1}\eta_h$$

$$\eta_1\eta_{h+1}\eta_{k+1} = n^{(k)}.f.\eta_{h+1} + m_0^k.\eta_1\eta_{h+1} + m_1^k.\eta_2\eta_{h+1} + \ldots + m_{e-1}^k\eta_0\eta_{h+1}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\eta_{e-1}\eta_{h-1}\eta_{k-1} = n^{(k)}.f.\eta_{h-1} + m_0^k.\eta_{e-1}\eta_{h-1} + m_1^k.\eta_0\eta_{h-1} + \ldots$$
$$+ m_{e-1}^k.\eta_{e-2}\eta_{h-1}.$$

Addirt man diese Gleichungen, so wird der Coëfficient von $n^{(k)}$ sowie der Coëfficient jeder der Zahlen m_i^k nach (8) den Werth $-f$ haben, ausgenommen für ein gerades f den Coëfficienten von m_h^k, welcher

$$\eta_h\eta_h + \eta_{h+1}\eta_{h+1} + \ldots + \eta_{h-1}\eta_{h-1}$$

also nach (5) gleich $p-f$ wird, da, wenn f gerade, $n^{(0)}=1$ ist; für ein ungerades f aber den Coëfficienten $m_{h+\frac{e}{2}}^k$, welcher

$$\eta_h\eta_{h+\frac{e}{2}} + \eta_{h+1}\eta_{h+\frac{e}{2}+1} + \ldots + \eta_{h-1}\eta_{h-1+\frac{e}{2}}$$

ist, also denselben Werth hat, weil jetzt $n^{\left(\frac{e}{2}\right)}=1$ ist. Je nach diesen beiden Fällen für f ergiebt sich also bei Berücksichtigung der Gleichung (6):

$$(9)\begin{cases} \text{wenn } f \text{ gerade ist, } \eta_0\eta_h\eta_k + \eta_1\eta_{h+1}\eta_{k+1} + \ldots \\ \qquad + \eta_{e-1}\eta_{h-1}\eta_{k-1} = -f^2 + p.m_h^k \\ \text{wenn } f \text{ ungerade ist, } \eta_0\eta_h\eta_k + \eta_1\eta_{h+1}\eta_{k+1} + \ldots \\ \qquad + \eta_{e-1}\eta_{h-1}\eta_{k-1} = -f^2 + p.m_{h+\frac{e}{2}}^k. \end{cases}$$

Da nun der Ausdruck zur Linken dieser Gleichungen durch eine Vertauschung von h und k sich nicht ändert, so erhält man eine weitere Eigenschaft der Zahlen m_h^k, welche durch die Gleichungen

$$(10)\qquad \begin{cases} m_h^k = m_k^h \text{ für ein gerades } f \\ m_{h+\frac{e}{2}}^k = m_{k+\frac{e}{2}}^h \text{ für ein ungerades } f \end{cases}$$

ausgedrückt wird.

Endlich setze man in Gleichung (5) statt der Zahlen m und k resp. $m+k$ und $e-k$, so ergiebt sich

$$\eta_m\eta_{m+k} = n^{(e-k)}.f + m_0^{e-k}.\eta_{m+k} + m_1^{e-k}.\eta_{m+k+1} + \ldots + m_{e-1}^{e-k}.\eta_{m+k-1};$$

die Vergleichung dieses Werthes von $\eta_m\eta_{m+k}$ mit dem durch (5)

gegebenen liefert aber mit Leichtigkeit noch folgende Beziehung zwischen den Zahlen m_h^k:

(11) $$m_h^k = m_{h-k}^{e-k}\,.$$

2. Nach diesen Vorbereitungen wollen wir nun zunächst diejenige quadratische Gleichung aufstellen, welche die $\frac{p-1}{2}$-gliedrigen Perioden zu Wurzeln hat; sind diese η_0, η_1, so sind also in der Gleichung

$$x^2 - (\eta_0 + \eta_1)\,x + \eta_0\eta_1 = 0$$

die Coëfficienten zu bestimmen. Nun ist nach Gleichung (1)

$$\eta_0 + \eta_1 = -1,$$

nach Gleichung (4) aber, wenn $\frac{p-1}{2}$, was hier an Stelle von f tritt, gerade ist,

$$\eta_0\eta_1 = m'_0\eta_0 + m'_1\eta_1\,.$$

Die ganzen Zahlen m'_0, m'_1 ergeben sich nach Formel (11) einander gleich, was man auch leicht durch folgende Betrachtung erkennt. Nennt man n den Werth von $\eta_0 . \eta_1$, welcher nach Nr. 6, 3) der 6. Vorlesung eine ganze Zahl ist, so lässt sich die vorige Gleichung auch so schreiben:

$$(m'_0 + n)\,\eta_0 + (m'_1 + n)\,\eta_1 = 0\,,$$

in welcher Gleichung man alle Potenzen von r unter den p^{ten} Grad erniedrigen, sodann durch r dividiren und so eine Gleichung erhalten kann, welche wegen der Irreductibilität der Kreistheilungsgleichung $m'_0 = m'_1 = -n$ ergiebt. Dieses Resultat, verbunden mit der aus (6) folgenden Bedingung $m'_0 + m'_1 = \frac{p-1}{2}$ liefert

$$\eta_0\eta_1 = -\frac{p-1}{4}\,.$$

Ist dagegen $\frac{p-1}{2}$ ungerade, so findet sich aus Gleichung (4)

$$\eta_0\eta_1 = \frac{p-1}{2} + m'_0\eta_0 + m'_1\eta_1$$

und auf demselben Wege die Gleichheit der Coëfficienten m'_0, m'_1, welche wegen der aus (6) folgenden Bedingung

$$1 + m'_0 + m'_1 = \frac{p-1}{2}$$

die Gleichungen $m'_0 = m'_1 = \frac{p-3}{4}$ und

$$\eta_0\,\eta_1 = \frac{p+1}{4}$$

liefert. Beide Fälle lassen sich in einer Formel zusammenfassen, indem man schreibt

$$\eta_0\eta_1 = \frac{1-(-1)^{\frac{p-1}{2}}.p}{4}.$$

Die gesuchte Gleichung hat demnach die Form:

$$(12)\qquad x^2 + x + \frac{1-(-1)^{\frac{p-1}{2}}.p}{4} = 0,$$

und ihre Wurzeln sind

$$(13)\qquad \eta_0 = \frac{-1+\sqrt{(-1)^{\frac{p-1}{2}}p}}{2},\quad \eta_1 = \frac{-1-\sqrt{(-1)^{\frac{p-1}{2}}p}}{2},$$

wie uns bereits durch die Formeln (26) der 9. Vorlesung bekannt ist, von wo wir sogar noch weiter wissen, dass die Quadratwurzeln in diesen Formeln positiv zu nehmen sind, sobald unter r die Wurzel $\cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$ verstanden wird. Setzt man $y = 2x + 1$, so nimmt die Gleichung (12) die einfachere Gestalt an:

$$(14)\qquad y^2 = (-1)^{\frac{p-1}{2}}.p. —$$

Da für ein gerades $\frac{p-1}{2}$, d. h. für eine Primzahl von der Form $4n+1$ sich $n^{(1)} = 0$ ergiebt, so findet die Congruenz (2) d. h., da $e = 2$, $k = 1$ zu setzen ist, die folgende:

$$(15)\qquad g^{2t+1} \equiv -1 \pmod{p}$$

für keinen Werth des t statt, und folglich muss -1 einer geraden Potenz von g congruent, also quadratischer Rest von p sein. Ist dagegen p von der Form $4n+3$ also $\frac{p-1}{2}$ ungerade, so findet die Congruenz (2) für $e = 2$, $k = 1$ d. i. die Congruenz (15) statt, wenn man $t = \frac{p-3}{4}$ setzt, also ist -1 quadratischer Nichtrest von p. Man gelangt auf diesem Wege wieder zu der Formel

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

zurück, welche in Nr. 2 der 9. Vorlesung aus der Theorie der quadratischen Reste direct gefunden ist.

3. Nach Nr. 8 der 6. Vorlesung sind die $\frac{p-1}{2}$ Einheitswurzeln, aus welchen die Periode η_0 besteht, die Wurzeln einer Gleichung vom Grade $\frac{p-1}{2}$, deren Coëfficienten ganze, lineare und ganzzahlige Functionen der beiden Perioden η_0, η_1 sind, also die Form $a_0\eta_0 + a_1\eta_1$ oder nach den Formeln (13) auch folgende Form:

$$\frac{m + n\sqrt{(-1)^{\frac{p-1}{2}} p}}{2}$$

haben, während darin die Coëfficienten ganze Zahlen bedenten. Bezeichnen wir jene Gleichung kurz durch

$$z = x^{\frac{p-1}{2}} + M_1 x^{\frac{p-3}{2}} + \ldots + M_{\frac{p-1}{2}} = 0,$$

so ist hiernach klar, dass wir setzen dürfen:

$$z = \frac{Y(x) + Z(x) \,.\, \sqrt{(-1)^{\frac{p-1}{2}} p}}{2},$$

wenn unter $Y(x)$, $Z(x)$ gewisse ganze Functionen von x mit ganzzahligen Coëfficienten verstanden werden. Die Gleichung $z' = 0$ aber, welcher die, die andere Periode η_1 zusammensetzenden, Einheitswurzeln genügen, erhält man offenbar aus der Gleichung $z = 0$, indem man in den Coëfficienten dieser-letzteren r durch r^g ersetzt d. i. η_0 mit η_1 vertauscht, oder auch, was nach den Formeln (13) auf Dasselbe hinausläuft, indem man das Vorzeichen der Quadratwurzel in das entgegengesetzte verwandelt. So findet man

$$z' = \frac{Y(x) - Z(x) \,.\, \sqrt{(-1)^{\frac{p-1}{2}} \,.\, p}}{2}.$$

Da nun die Function $X = \frac{x^p - 1}{x - 1}$ in das Product der beiden Factoren z, z' zerfällt, so ergiebt sich mittels Substitution folgende merkwürdige Formel:

$$(16) \qquad 4 \cdot \frac{x^p - 1}{x - 1} = Y(x)^2 - (-1)^{\frac{p-1}{2}} p \cdot Z(x)^2 .$$

In welcher Weise die Functionen $Y(x)$, $Z(x)$ zusammengesetzt sind, darüber wollen wir hier nur einige einfache Bemerkungen beifügen. Ohne Weiteres lässt sich soviel übersehen, dass, weil

$$M_1 = -\eta_0 = \frac{1 - \sqrt{(-1)^{\frac{p-1}{2}} \cdot p}}{2}$$

ist, die höchsten Glieder der Functionen $Y(x)$, $Z(x)$ resp. $2x^{\frac{p-1}{2}} + x^{\frac{p-3}{2}}$, $-x^{\frac{p-3}{2}}$ sein müssen. — Bezeichnet man ferner mit $A(x)$ den Ausdruck

$$\tfrac{1}{2}\left(Y(x) + \sqrt{\varepsilon p} \cdot Z(x)\right),$$

mit $B(x)$ den Ausdruck

$$\tfrac{1}{2}\left(Y(x) - \sqrt{\varepsilon p} . Z(x)\right),$$

wo ε zur Abkürzung für $(-1)^{\frac{p-1}{2}}$ gesetzt ist, so ist

$$A(x) = \prod_\alpha (x - r^\alpha), \quad B(x) = \prod_\beta (x - r^\beta),$$

wenn mit α, β z. B. alle diejenigen quadratischen Reste und Nichtreste von p bezeichnet werden, welche kleiner als p sind. Die letzten Coëfficienten dieser beiden Functionen sind $(-1)^{\frac{p-1}{2}} . r^{\Sigma\alpha}$ und $(-1)^{\frac{p-1}{2}} . r^{\Sigma\beta}$ oder einfacher gleich $(-1)^{\frac{p-1}{2}}$, da $\Sigma\alpha$ und $\Sigma\beta$ durch p theilbar sind, wie man sofort einsieht, wenn man bemerkt, dass

$$\left.\begin{array}{l} \Sigma\alpha \equiv 1 + g^2 + g^4 + \ldots\ldots + g^{p-3} \\ \Sigma\beta \equiv g\,(1 + g^2 + g^4 + \ldots\ldots + g^{p-3}) \end{array}\right\} \pmod{p},$$

und die Summe $1 + g^2 + g^4 + \ldots\ldots + g^{p-3} = \frac{g^{p-1} - 1}{g^2 - 1} \equiv 0$ (mod. p) ist.

Will man nun aus der Gleichung $A(x) = 0$, welche die Wurzeln r^α hat, zu der Gleichung übergehen, welche die reciproken Werthe $r^{-\alpha}$ zu Wurzeln hat, so hat man bekanntlich x in $\frac{1}{x}$ zu

verwandeln, wodurch sich die Gleichung $A\left(\frac{1}{x}\right)=0$ ergiebt, welche man jedoch, wenn nur ganze Potenzen von x darin auftreten und das höchste Glied den Coëfficienten Eins haben soll, mit $(-1)^{\frac{p-1}{2}}\cdot x^{\frac{p-1}{2}}$ zu multipliciren hat. Daraus ergiebt sich offenbar die Gleichung

$$(-x)^{\frac{p-1}{2}}\cdot A\left(\frac{1}{x}\right)=\prod_{\alpha}(x-r^{-\alpha})$$

und auf demselben Wege

$$(-x)^{\frac{p-1}{2}}\cdot B\left(\frac{1}{x}\right)=\prod_{\beta}(x-r^{-\beta})\,.$$

Unterscheiden wir nun die beiden Fälle, in denen p von der Form $4n+1$ und von der Form $4n+3$ ist. Im ersten stimmen die Reste der Zahlen $-\alpha$ (mod. p) mit den Zahlen α, die Reste der Zahlen $-\beta$ mit den Zahlen β überein, da -1 quadratischer Rest von p ist. Daher ergiebt sich

$$x^{\frac{p-1}{2}}\cdot A\left(\frac{1}{x}\right)=A(x),\; x^{\frac{p-1}{2}}\cdot B\left(\frac{1}{x}\right)=B(x)$$

d. h.

$$x^{\frac{p-1}{2}}\cdot\left[Y\left(\frac{1}{x}\right)+\sqrt{\varepsilon p}\cdot Z\left(\frac{1}{x}\right)\right]=Y(x)+\sqrt{\varepsilon p}\cdot Z(x),$$

also

$$(17)\qquad x^{\frac{p-1}{2}}\cdot Y\left(\frac{1}{x}\right)=Y(x),\; x^{\frac{p-1}{2}}\cdot Z\left(\frac{1}{x}\right)=Z(x)\,.$$

Im zweiten Falle stimmen, da dann -1 quadratischer Nichtrest von p ist, die Reste der Zahlen $-\alpha$ (mod. p) mit den Zahlen β, die Reste von $-\beta$ (mod. p) mit den Zahlen α überein, wodurch man findet:

$$-x^{\frac{p-1}{2}}\cdot A\left(\frac{1}{x}\right)=B(x),\; -x^{\frac{p-1}{2}}\cdot B\left(\frac{1}{x}\right)=A(x)$$

d. h.

$$x^{\frac{p-1}{2}}\left[Y\left(\frac{1}{x}\right)+\sqrt{\varepsilon p}\cdot Z\left(\frac{1}{x}\right)\right]=-Y(x)+\sqrt{\varepsilon p}\cdot Z(x)$$

also

$$(18) \qquad x^{\frac{p-1}{2}} \cdot Y\left(\frac{1}{x}\right) = - Y(x), \; x^{\frac{p-1}{2}} \cdot Z\left(\frac{1}{x}\right) = Z(x) \, .$$

Die Gleichungen (17) und (18) bedingen zwischen den Coëfficienten der Functionen $Y(x)$, $Z(x)$ gewisse Beziehungen, auf welche wir bei einer späteren Gelegenheit werden Rücksicht zu nehmen haben.†)

Andere Bemerkungen über die Zusammensetzung der Functionen $Y(x)$, $Z(x)$, auf die hier einzugehen nicht weiter erforderlich ist, sind von Legendre*) später auch von Liouville**) und v. Staudt***) angegeben worden, auf deren Arbeiten wir hier den Leser verweisen.

Noch eine andere wichtige Folgerung aber können wir an die Gleichung $z = 0$ knüpfen, welche zur Ergänzung der Theorie der quadratischen Reste dient, indem sie uns den quadratischen Charakter der Zwei liefert.

Bemerken wir im Voraus, dass die Coëfficienten der Gleichung $z = 0$ mittels der Newton'schen Formeln aus den Potenzsummen ihrer Wurzeln gefunden werden können, welche letztere leicht angebbar sind. Setzt man wieder

$$S = \sum_{\alpha} r^{\alpha} - \sum_{\beta} r^{\beta} = + \sqrt{(-1)^{\frac{p-1}{2}} \cdot p} \, ,$$

also $\sum_{\alpha} r^{\alpha} = \frac{1}{2}(-1 + S)$, so ergiebt sich aus den beiden Gleichungen

$$\sum_{\alpha} r^{k\alpha} + \sum_{\beta} r^{k\beta} = -1, \quad \sum_{\alpha} r^{k\alpha} - \sum_{\beta} r^{k\beta} = S_k = \left(\frac{k}{p}\right) S,$$

in welchen k durch p nicht theilbar vorausgesetzt ist, die Summe der k^{ten} Potenzen von den Wurzeln jener Gleichung, nämlich

$$\sum_{\alpha} r^{k\alpha} = \frac{1}{2}\left[-1 + \left(\frac{k}{p}\right) \cdot S\right].$$

---

†) Vgl. Dirichlet's Vorlesungen über Zahlentheorie, herausg. von Dedekind, § 140.

*) Legendre, théorie des nombres, 2. édit. Nr. 478.

**) Liouville, sur un point de la théorie des équations binômes, in s. Journal Bd. 4, 2. série.

***) v. Staudt in einer Abhandlung in Cr. J. Bd. 67 pag. 205.

Betrachten wir nun besonders den zweiten Coëfficienten der Gleichung, für welchen man nach den Newton'schen Formeln bekanntlich

$$2 \cdot M_2 = \left(\sum_\alpha r^\alpha\right)^2 - \sum r^{2\alpha}$$

hat, während

$$\sum_\alpha r^{2\alpha} = \tfrac{1}{2}\left[-1 + \left(\frac{2}{p}\right) \cdot S\right]$$

ist, so müssen nach Nr. 8 der 6. Vorl. alle Coëfficienten in der Differenz, wenn sie so reducirt wird, dass sie kein von r unabhängiges Glied mehr enthält, gerade Zahlen sein. Man findet aber

$$\left(\sum_\alpha r^\alpha\right)^2 - \sum_\alpha r^{2\alpha} = \frac{3 + (-1)^{\frac{p-1}{2}} \cdot p}{4} - \tfrac{1}{2}\left[1 + \left(\frac{2}{p}\right)\right] S$$

$$= \left[\frac{1}{2}\left[1 + \left(\frac{2}{p}\right)\right] - \frac{3 + (-1)^{\frac{p-1}{2}} \cdot p}{4}\right] \cdot \sum_\beta r^\beta$$

$$- \left[\frac{1}{2}\left[1 + \left(\frac{2}{p}\right)\right] + \frac{3 + (-1)^{\frac{p-1}{2}} \cdot p}{4}\right] \cdot \sum_\alpha r^\alpha.$$

Da hierin die Coëfficienten gerade Zahlen sein sollen, muss

$$2\left[1 + \left(\frac{2}{p}\right)\right] \equiv 3 + (-1)^{\frac{p-1}{2}} \cdot p \pmod{8}$$

sein, aus welcher Congruenz man für $p = 8n + 1$ und $p = 8n + 7$ die Gleichung $\left(\frac{2}{p}\right) = +1$, dagegen für $p = 8n + 3$ und $p = 8n + 5$ die Gleichung $\left(\frac{2}{p}\right) = -1$ erschliesst. So ergiebt sich folgender Satz:

Die 2 ist quadratischer Rest von allen Primzahlen einer der beiden Formen $8n \pm 1$, dagegen quadratischer Nichtrest von allen Primzahlen der Formen $8n \pm 3$, ein Satz, den man leicht durch folgende Gleichung ausdrückt:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{19}$$

4. Setzen wir jetzt p als eine Primzahl von der Form $6n + 1$ voraus, so können wir drei Perioden

von $\frac{p-1}{3}$ Gliedern bilden und nach der cubischen Gleichung fragen, welche sie zu Wurzeln hat. Diese steht zur Theorie der cubischen Reste in derselben Beziehung, wie die vorher betrachtete quadratische Gleichung zur Lehre von den quadratischen Resten, und bietet daher in mehrfacher Beziehung Interesse dar. Sind η_0, η_1, η_2 die drei $\frac{p-1}{3}$-gliedrigen Perioden, so handelt es sich darum, die Werthe der Coëfficienten in der cubischen Gleichung

(20) $x^3-(\eta_0+\eta_1+\eta_2)x^2+(\eta_0\eta_1+\eta_1\eta_2+\eta_2\eta_0)x-\eta_0\eta_1\eta_2=0$

zu bestimmen. Da hier $f=\frac{p-1}{3}$ gerade ist, so liefern die Gleichungen (1) und (7) sogleich die Werthe der beiden ersten:

$$\eta_0+\eta_1+\eta_2=-1$$

$$\eta_0\eta_1+\eta_1\eta_2+\eta_2\eta_0=-\frac{p-1}{3}.$$

Setzt man sodann in der ersten der Gleichungen (9) $k=1$, $h=2$, so ergiebt sich auch der dritte Coëfficient durch die Gleichung:

$$(21)\qquad 3\,.\,\eta_0\eta_1\eta_2=-\left(\frac{p-1}{3}\right)^2+p\,.\,m'_2.$$

Da jedoch auf diesem Wege eine merkwürdige Beziehung, welche die ganzen Zahlen m_h^k in diesem Falle zur Theorie der cubischen Reste darbieten, nicht hervortritt, soll derselbe Coëfficient noch auf einem andern Wege ermittelt werden.

Dazu bemerke man zunächst, dass das Schema der neun Werthe

$$(22)\qquad \begin{cases} m_0{}^0 & m_1{}^0 & m_2{}^0 \\ m_0{}^1 & m_1{}^1 & m_2{}^1 \\ m_0{}^2 & m_1{}^2 & m_2{}^2 \end{cases}$$

sich mit Rücksicht auf die in Nr. 1 angegebenen Eigenschaften (10) und (11) der Zahlen m_h^k auf das folgende reducirt, welches nur noch vier verschiedene Werthe enthält:

$$(23)\qquad \begin{cases} m_0{}^0 & m_1{}^0 & m_2{}^0 \\ m_1{}^0 & m_2{}^0 & m_2{}^1 \\ m_2{}^0 & m_2{}^1 & m_1{}^0. \end{cases}$$

Multiplicirt man nun die aus (5) für $m = k = 1$ sich ergebende Gleichung

$$\eta_1 \eta_2 = m_0^1 \eta_1 + m_1^1 \eta_2 + m_2^1 \eta_0$$

mit η_0 und setzt für die Producte $\eta_0 \eta_0$, $\eta_0 \eta_1$, $\eta_0 \eta_2$ ihre durch dieselbe Formel gegebenen Werthe ein, so wird man finden:

$$\eta_0 \eta_1 \eta_2 = m_2^1 . f + [m_0^0 m_2^1 + (m_1^0)^2 + (m_2^0)^2] \eta_0 \\ + [m_1^0 m_2^0 + m_2^0 m_2^1 + m_2^1 m_1^0] (\eta_1 + \eta_2).$$

Da aber $\eta_0 \eta_1 \eta_2$ nach Nr. 6, 3) der 6. Vorlesung eine ganze Zahl ist, müssen auf der rechten Seite dieser Gleichung die Coëfficienten der einzelnen Perioden einander gleich sein, wodurch dann

$$\eta_0 \eta_1 \eta_2 = m_2^1 . f - (m_1^0 m_2^0 + m_2^0 m_2^1 + m_2^1 m_1^0),$$

oder wegen der Gleichung

$$m_0^2 + m_1^2 + m_2^2 = m_2^0 + m_2^1 + m_1^0 = f:$$

(24) $$\eta_0 \eta_1 \eta_2 = (m_2^1)^2 - m_1^0 m_2^0$$

hervorgeht.

Hiernach bestehen zwischen den vier Zahlen m_0^0, m_1^0, m_2^0, m_2^1 drei Gleichungen, nämlich nach (6) die beiden Gleichungen:

(25) $$\begin{cases} m_0^0 + m_1^0 + m_2^0 = f - 1 \\ m_1^0 + m_2^0 + m_2^1 = f \end{cases}$$

aus welchen

(26) $$m_0^0 = m_2^1 - 1$$

sich ergiebt, und nach der eben gemachten Bemerkung noch die folgende:

(27) $$m_2^1 (m_2^1 - 1) + (m_1^0)^2 + (m_2^0)^2 = m_1^0 m_2^0 + m_2^0 m_2^1 + m_2^1 m_1^0.$$

Es ereignet sich nun merkwürdiger Weise, dass die drei Gleichungen (25) und (27), verbunden mit der Bedingung, dass die Zahlen m_h^k ganze Zahlen sind, vollständig zur Bestimmung der vier Coëfficienten ausreichen, wie man sofort sieht, indem man der vorigen mit 36 multiplicirten Gleichung nachstehende Form ertheilt:

$$12 m_2^1 + 12 m_1^0 + 12 m_2^0 + 4 = 36 (m_2^1)^2 + 9 (m_1^0 + m_2^0)^2 \\ + 4 - 36 m_2^1 (m_1^0 + m_2^0) - 24 m_2^1 + 12 (m_1^0 + m_2^0) + 27 (m_1^0 - m_2^0)^2,$$

aus welcher, mit Benutzung der Gleichung $m_1^0 + m_2^0 + m_2^1 = \frac{p-1}{3}$ sich die Relation:

(28) $4p = (6m_2^1 - 3m_1^0 - 3m_2^0 - 2)^2 + 27(m_1^0 - m_2^0)^2$
ergiebt.

Man gelangt auf diese Weise einerseits zu dem bereits in Nr. 1 der 11. Vorlesung gefundenen Satze, dass das Vierfache einer Primzahl von der Form $6n + 1$ stets als Summe eines einfachen Quadrates und eines dreifachen Quadrates dargestellt werden kann, deren Basis resp. der Eins und der Null (mod. 3) congruent sind, wieder zurück. Andererseits liefert gerade der Umstand, dass eine solche Zerlegung, wie aus dem Hauptsatze der Nr. 2 voriger Vorlesung hervorgeht, nur auf eine Weise möglich ist, eine genaue Bestimmung der Coëfficienten m_1^0, m_2^0, m_0^0, m_2^1, indem sich die eine Gleichung (28) dadurch in zwei andere zerlegt. In der That, bezeichnen A, B dieselben Zahlen, wie in der angeführten Stelle der 11. Vorlesung, so muss

(29) $6m_2^1 - 3m_1^0 - 3m_2^0 - 2 = A, \; 3(m_1^0 - m_2^0) = B$

sein. Man könnte zweifelhaft sein, ob B in der zweiten dieser Gleichungen nicht negativ zu nehmen sei; der Natur der Sache nach ist weder das Zeichen von B noch auch das von $m_1^0 - m_2^0$ völlig bestimmt, sondern von der Wahl der primitiven Wurzel g abhängig, bei deren Veränderung die Perioden η_1, η_2, also auch die Zahlen m_1^0, m_2^0 sich mit einander vertauschen können. Dass aber die beiderseitigen Vorzeichen auf die in (29) angenommene Weise einander entsprechen, soll sogleich durch eine andere Betrachtung erhärtet werden.

Nun können die Werthe der vier Coëfficienten $m_0^0, m_1^0, m_2^0, m_2^1$ bestimmt werden. Setzt man $A = 3\alpha - 2$, $B = 3\beta$, so findet man zunächst aus den beiden Gleichungen

$$\alpha = 2m_2^1 - m_1^0 - m_2^0, \; f = m_2^1 + m_1^0 + m_2^0$$

unmittelbar:

$$m_2^1 = \frac{\alpha + f}{3},$$

also nach (26):

$$m_0^0 = \frac{\alpha + f - 3}{3},$$

sodann aus den beiden Gleichungen

$$m_1^0 + m_2^0 = 2m_2^1 - \alpha, \; m_1^0 - m_2^0 = \beta$$

die beiden andern Werthe:

$$m_1{}^0 = \frac{2f + 3\beta - \alpha}{6}, \quad m_2{}^0 = \frac{2f - 3\beta - \alpha}{6}.$$

Hierauf ergiebt sich, da $f = \frac{p-1}{3}$ ist, vermittelst der Gleichung (21) folgender Werth des noch zu bestimmenden dritten Coëfficienten der cubischen Gleichung:

$$(30) \qquad \eta_0 \eta_1 \eta_2 = \frac{1}{9}\left(p\alpha + \frac{p-1}{3}\right).$$

Demnach nimmt endlich die gesuchte cubische Gleichung die Gestalt*) an:

$$(31) \qquad x^3 + x^2 - \frac{p-1}{3}x - \frac{1}{9}\left(p\alpha + \frac{p-1}{3}\right) = 0,$$

oder, vermittelst der Substitution $3x + 1 = y$, die einfachere Form:

$$(32) \qquad y^3 - 3py - pA = 0.$$

5. Da die merkwürdige Beziehung, welche die Coëfficienten m_h^k zu der Darstellung von $4p$ in der Form $A^2 + 3B^2$ gezeigt haben, bei der eben geführten Untersuchung ganz überraschend auftrat, wollen wir, ehe wir zu andern Betrachtungen weitergehen, ihren Grund aufsuchen. Derselbe liegt aber in dem Umstande, dass diese Coëfficienten mit der Function $\psi(h, k, g)$ zusammenhängen, welche wir in Nr. 2 der 10. Vorlesung eingeführt haben. In der That, die Congruenz

$$\psi(h, k, g) \equiv \sum_{\mu=1}^{\mu=p-2} \mu^h (\mu + 1)^n \pmod{p}$$

kann man auch so schreiben:

$$\psi(h, k, g) \equiv \sum g^{hm} (g^m + 1)^n \pmod{p},$$

wo m alle Werthe von 0 bis $p - 2$ mit Ausnahme des Werthes $\frac{p-1}{2}$ anzunehmen hat, oder, wenn man $m = et + u$ setzt, und, damit m seine Werthe durchläuft, t alle Zahlen $0, 1, 2, \ldots . f - 1$, u aber alle Zahlen $0, 1, 2, \ldots . e - 1$ durchlaufen lässt, die-

---

*) Vgl. Gauss' disquis. arithm. art. 358. Auch Lebesgue, recherches sur les nombres in Liouv. J. Bd. 3.

jenige Combination t, u ausgenommen, für welche $m = u + et = \frac{p-1}{2}$ würde, auch folgendermassen:

$$\psi(h, k, g) \equiv \sum g^{(u+et)h} \cdot (g^{u+et} + 1)^n. \quad (\text{mod. } p).$$

Betrachten wir zuerst den Theil dieser Summe, welcher einem bestimmten Werthe des u entspricht, also die Summe:

$$\sum_t g^{(u+et)h} \cdot (g^{u+et} + 1)^n,$$

so enthält diese kein Glied, für welches $g^{u+et} + 1 \equiv 0$ (mod. p) wäre; bezeichnet daher wieder m_v^u die Anzahl der Werthe von t, für welche die Congruenz

$$g^{u+et} + 1 \equiv g^{v+ez} \quad (\text{mod. } p)$$

stattfindet, während v aus der Reihe $0, 1, 2, \ldots . e-1$ ist, so wird jene Summe (mod. p) der folgenden:

$$\sum m_v^u \cdot g^{uh+vn+e(ht+nz)},$$

in den Fällen also, wo h und n als Vielfache von f vorausgesetzt werden, auch der nächsten:

$$\sum m_v^u \cdot g^{uh+vn}$$

congruent, und folglich

$$\psi(h, k, g) \equiv \sum_{u,v} m_v^u \cdot g^{uh+vn} \quad (\text{mod. } p), \tag{33}$$

worin die Summation in Bezug auf u und v über alle Werthe aus der Reihe $0, 1, 2, \ldots . e-1$ zu erstrecken ist. Da bei diesen Transformationen die Anzahl der Glieder in den Summen sich nicht geändert hat, so ergiebt sich die Gleichung

$$\sum_{u,v} m_v^u = p - 2. \tag{34}$$

Bisher hatten wir keine Annahme über die Form der Primzahl p noch über die Art der Zerlegung von $p-1$ in die Factoren e, f zu machen; nunmehr wollen wir voraussetzen, p sei von der Form $6n+1$, $e = 3$, $f = \frac{p-1}{3}$. Setzt man dann $h = n = f$, so geht $\psi(h, k, g)$ in die Function $\psi\left(\frac{p-1}{3}, \frac{p-1}{3}, g\right)$ über, für welche nach den Bezeichnungen in Nr. 3 der 11. Vor-

lesung die Congruenz besteht:

$$\psi\left(\frac{p-1}{3}, \frac{p-1}{3}, g\right) \equiv A_0 + A_1 g^{\frac{p-1}{3}} + A_2 g^{2.\frac{p-1}{3}} \quad (\text{mod. } p).$$

Die Formel (33) liefert also

$$(35)\quad B_0 + B_1 . g^{\frac{p-1}{3}} + B_2 . g^{2\frac{p-1}{3}} = A_0 + A_1 . g^{\frac{p-1}{3}} + A_2 . g^{2\frac{p-1}{3}} \quad (\text{mod. } p),$$

wenn

$$\sum_{u,v} m_v^u . g^{(u+v)f} \equiv B_0 + B_1 g^{\frac{p-1}{3}} + B_2 g^{2\frac{p-1}{3}}$$

d. h.

$$B_0 = \sum_{u,v}{}^{0} m_v^u,\ B_1 = \sum_{u,v}{}' m_v^u,\ B_2 = \sum_{u,v}{}'' m_v^u$$

gesetzt, und diese drei Summen über alle Combinationen u, v bezogen werden, für welche resp. $u + v \equiv 0, 1, 2 \pmod{3}$ ist. Nach Gleichung (34) besteht sodann die Gleichung

$$(36)\qquad B_0 + B_1 + B_2 = p - 2.$$

Setzt man dagegen $h = n = 2f$, so geht die Function $\psi(h, k, g)$ in die Function $\psi\left(2.\frac{p-1}{3}, 2.\frac{p-1}{3}, g\right)$ über, für welche

$$\psi\left(2\frac{p-1}{3}, 2\frac{p-1}{3}, g\right) \equiv A_0 + A_1 . g^{2\frac{p-1}{3}} + A_2 . g^{\frac{p-1}{3}} \quad (\text{mod. } p)$$

war. Die Formel (33) liefert also bei derselben Substitution:

$$(37)\qquad \sum_{u,v} m_v^u . g^{(u+v)2f} \equiv B_0 + B_1 . g^{2\frac{p-1}{3}} + B_2 . g^{\frac{p-1}{3}}$$

$$\equiv A_0 + A_1 . g^{2\frac{p-1}{3}} + A_2 . g^{\frac{p-1}{3}}.$$

Endlich giebt die Gleichung (36) in Verbindung mit der Gleichung

$$(38)\qquad A_0 + A_1 + A_2 = p - 2$$

(s. Nr. 3 der 11. Vorlesung) die Congruenz

$$B_0 + B_1 + B_2 \equiv A_0 + A_1 + A_2 \quad (\text{mod. } p),$$

welche zusammen mit (35) und (37) die Identität der Zahlen B_0, B_1, B_2 mit den Zahlen A_0, A_1, A_2 resp. erweist. Denn man findet leicht daraus

$$A_0 \equiv B_0,\ A_1 \equiv B_1,\ A_2 \equiv B_2 \quad (\text{mod. } p);$$

da aber sowohl die positiven ganzen Zahlen A_0, A_1, A_2 der Gleichung (38) wegen, als auch die positiven ganzen Zahlen B_0, B_1, B_2 wegen (36) kleiner als p sein müssen, so ergiebt sich

$$A_0 = B_0,\ A_1 = B_1,\ A_2 = B_2.$$

Bezeichnen nach alle Diesem a, b, A, B dieselben Zahlen wie in der 11. Vorlesung, nämlich

$$a = A_0 - A_2,\ b = A_1 - A_2,\ A = 2a - b,\ B = b,$$

so findet man, mit Rücksicht auf die Bedeutung der Zahlen B_0, B_1, B_2:

$$a = m_0{}^0 + m_2{}^1 + m_1{}^2 - m_2{}^0 - m_1{}^1 - m_0{}^2,$$
$$b = m_1{}^0 + m_0{}^1 + m_2{}^2 - m_2{}^0 - m_1{}^1 - m_0{}^2$$

oder nach den Eigenschaften der Zahlen m_h^k:

$$a = m_0{}^0 + 2m_2{}^1 - 3m_2{}^0,\ b = 3(m_1{}^0 - m_2{}^0)$$

also

$$A = 6m_2{}^1 - 3(m_2{}^0 + m_1{}^0) - 2,\ B = 3(m_1{}^0 - m_2{}^0),$$

wie vorher aus der Kreistheilung gefunden worden ist.

6. **Die Wurzeln der Gleichung (31) sind nach den Formeln (12) der 14. Vorlesung leicht anzugeben.** Da ϱ^m den Werthen 1, ϱ, ϱ^2 gleich ist, jenachdem $m \equiv 0, 1, 2 \pmod{3}$ ist, so findet man offenbar aus der Gleichung

$$T_1 = \sum_{m=0}^{m=p-2} \varrho^m \cdot r^{g^m}$$

die folgende:

$$T_1 = \eta_0 + \varrho\eta_1 + \varrho^2\eta_2$$

und ebenso:

$$T_2 = \eta_0 + \varrho^2\eta_1 + \varrho\eta_2,$$

aus welchen Gleichungen in Verbindung mit der Gleichung $-1 = \eta_0 + \eta_1 + \eta_2$ **für die drei Perioden folgende Werthe gefunden werden:**

$$\eta_0 = \tfrac{1}{3}(-1 + T_1 + T_2) = \tfrac{1}{3}\left(-1 + \sqrt[3]{p\varpi} + \sqrt[3]{p\varpi'}\right)$$
$$\eta_2 = \tfrac{1}{3}(-1 + \varrho T_1 + \varrho^2 T_2) = \tfrac{1}{3}\left(-1 + \varrho\sqrt[3]{p\varpi} + \varrho^2\sqrt[3]{p\varpi'}\right)$$
$$\eta_1 = \tfrac{1}{3}(-1 + \varrho^2 T_1 + \varrho T_2) = \tfrac{1}{3}\left(-1 + \varrho^2\sqrt[3]{p\varpi} + \varrho\sqrt[3]{p\varpi'}\right),$$

wo ϖ, ϖ' die primären Factoren von p und die beiden Cubikwurzeln, wegen der Gleichung (11) der vorigen Vorlesung, so zu wählen sind, dass ihr Product gleich p wird. **Setzt man**

$$\varepsilon_0 = 1 + 3\eta_0,\ \varepsilon_1 = 1 + 3\eta_1,\ \varepsilon_2 = 1 + 3\eta_2,$$

so werden $\varepsilon_0, \varepsilon_1, \varepsilon_2$ die Wurzeln der Gleichung (32) sein.

Obgleich die Werthe der Perioden η_0, η_1, η_2 unter imaginärer Form erscheinen, müssen sie doch, ebenso wie die Grössen $\varepsilon_0, \varepsilon_1, \varepsilon_2$, nach Nr. 11 der 6. Vorlesung reell sein. Dieser Umstand leuchtet auch folgendermassen leicht ein. Setzen wir $p = 6n + 1$, so ist $f = \frac{p-1}{3} = 2n$, also gerade. Wenn man nun

$$\eta_\alpha = r^{g^\alpha} + r^{g^{3+\alpha}} + r^{g^{6+\alpha}} + \ldots + r^{g^{3(2n-1)+\alpha}}$$

setzt, sodass man die drei Perioden η_0, η_1, η_2 erhält, wenn α successive gleich 0, 1, 2 gewählt wird, so kann man auch schreiben:

$$\eta_\alpha = \sum_{h=0}^{h=n-1} \left(r^{g^{3h+\alpha}} + r^{g^{3(n+h)+\alpha}}\right),$$

was in den Ausdruck

$$\eta_\alpha = \sum_{h=0}^{h=n-1} \left(r^{g^{3h+\alpha}} + r^{-g^{3h+\alpha}}\right)$$

übergeht, wenn man bemerkt, dass $g^{3n} \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ ist. Dieser Ausdruck ist aber offenbar reell; denn, da $r = \cos\frac{2\pi}{p} + i \sin\frac{2\pi}{p}$ ist, so wird das allgemeine Glied der Summe gleich

$$\left(\cos\frac{2\pi \cdot g^{3h+\alpha}}{p} + i\sin\frac{2\pi \cdot g^{3h+\alpha}}{p}\right) + \left(\cos\frac{2\pi \cdot g^{3h+\alpha}}{p} - i\sin\frac{2\pi \cdot g^{3h+\alpha}}{p}\right)$$
$$= 2 \cdot \cos\frac{2\pi \cdot g^{3h+\alpha}}{p},$$

also

$$\eta_\alpha = 2\sum_{h=0}^{h=n-1} \cos\frac{2\pi \cdot g^{3h+\alpha}}{p}.$$

Die vollständige Bestimmung der drei Perioden η_0, η_1, η_2 vermittelst der obigen Formeln, sowie die der Werthe $\varepsilon_0, \varepsilon_1, \varepsilon_2$ ist erst dann möglich, wenn die Frage gelöst ist, welchen der drei Werthe der Cubikwurzeln $\sqrt[3]{p\varpi}$ und $\sqrt[3]{p\varpi'}$ man für T_1 und T_2 resp. zu wählen hat, eine Frage, welche ihrer Lösung noch harrt, wie in der vorigen Vorlesung bemerkt worden ist. Könnte man umgekehrt angeben, welche der drei Wurzeln der Gleichung (32) mit $\varepsilon_0, \varepsilon_1, \varepsilon_2$ resp. zu bezeichnen sind, so würde sich daraus

diese Frage entscheiden lassen. Kummer hat in einer Abhandlung in Cr. J. Bd. 32 (de residuis cubicis disquisitiones nonnullae analyticae) auf diesem Wege die Lösung der Frage gesucht, ohne jedoch ganz zu dem gewünschten Ziele zu gelangen. Einige Bemerkungen über diese Arbeit werden hier am Orte sein. Man findet leicht, dass die Wurzeln der Gleichung (32) in den drei Intervallen:

von $-2\sqrt{p}$ bis $-\sqrt{p}$, von $-\sqrt{p}$ bis $+\sqrt{p}$, von $+\sqrt{p}$ bis $+2\sqrt{p}$

enthalten sind; denn, setzt man die Werthe $-2\sqrt{p}$, $-\sqrt{p}$, $+\sqrt{p}$, $+2\sqrt{p}$ successive für y in den Ausdruck

$$y^3 - 3py - pA$$

ein, so erhält man resp. die Werthe:

$$-p(2\sqrt{p}+A), -p(-2\sqrt{p}+A), -p(2\sqrt{p}+A), -p(-2\sqrt{p}+A),$$

welche zu zwei aufeinanderfolgenden multiplicirt das Product

$$p^2(A^2 - 4p)$$

d. h. mit Rücksicht auf die Gleichung $4p = A^2 - 3B^2$ den negativen Werth $-3p^2B^2$ liefern; es haben also je zwei aufeinanderfolgende jener Werthe entgegengesetztes Zeichen, woraus nach einem bekannten Satze der Algebra die Behauptung sich als richtig erweist. Alles kommt daher darauf an, zu entscheiden, in welchem der drei Intervalle die Wurzeln ε_0, ε_1, ε_2 resp. zu wählen sind. Diese Frage lehrt Kummer mittels analytischer Betrachtungen durch die Grössenfolge der drei Zahlen m_0, m_1, m_2 entscheiden, welche resp. die Summe derjenigen unter $\frac{p}{2}$ liegenden Zahlen bedeuten*), deren Indices den Resten 0, 1, 2 (mod. 3) congruent sind. Aber eine solche Beantwortung der Frage ist im Grunde nicht die gewünschte; denn, während man aus der Natur von p selbst eine Antwort darauf zu verlangen hat, sind die Zahlen m_0, m_1, m_2 so complicirte Functionen von p, dass man a priori über ihre Grössenfolge nichts aussagen kann, und für ein gegebenes p sind sie, sobald p etwas gross ist, nur mühsam zu berechnen.

Bei der Kummer'schen Untersuchung spielt besonders der Ausdruck

---

*) oder vielmehr gewisse sehr einfache Functionen dieser Summen.

$$(\varepsilon_0 - \varepsilon_1)(\varepsilon_1 - \varepsilon_2)(\varepsilon_2 - \varepsilon_0)$$

eine Rolle, dessen genauer Bestimmung auch Cauchy in Liouv. J., Bd. V eine besondere Abhandlung gewidmet hat. Bemerkt man, dass zwar η_0 und ε_0 von der willkürlichen Wahl der primitiven Wurzel g unabhängig sind, aber η_1 und η_2 untereinander, desgleichen also ε_1 und ε_2 unter einander vertauscht werden, wenn man die bestimmte primitive Wurzel durch eine passende andere ersetzt, so ist das Vorzeichen jenes Ausdrucks mit der Wahl der primitiven Wurzel in derselben Weise wechselnd, wie die Zahl B, sein genauer Werth wird also von dieser Zahl abhängig sein. Dies ist leicht zu bestätigen. Zunächst bemerke man die Gleichungen:

$$\varepsilon_0 + \varepsilon_1 + \varepsilon_2 = 0, \quad \varepsilon_1\varepsilon_2 + \varepsilon_2\varepsilon_0 + \varepsilon_0\varepsilon_1 = -3p, \quad \varepsilon_0\varepsilon_1\varepsilon_2 = pA,$$

zu denen man die folgende, als daraus folgend, hinzufügen kann:

$$\varepsilon_0^2 + \varepsilon_1^2 + \varepsilon_2^2 = 6p.$$

Bilden wir nun das Quadrat der Periode η_0, so finden wir nach den Kummer'schen Formeln, da $f = \frac{p-1}{3}$ gerade ist,

$$\eta_0^2 = \frac{p-1}{3} + m_0^0\eta_0 + m_1^0\eta_1 + m_2^0\eta_2,$$

also, wenn die Werthe für m_0^0, m_1^0, m_2^0 eingesetzt werden:

$$\eta_0^2 = f + \frac{2f-\alpha}{6}(\eta_0 + \eta_1 + \eta_2) + \frac{3\alpha - 6}{6}\eta_0 + \frac{3\beta}{6}(\eta_1 - \eta_2).$$

Da nun $\eta_0 + \eta_1 + \eta_2 = -1$ und $3(\eta_1 - \eta_2) = \varepsilon_1 - \varepsilon_2$ ist, kann man auch schreiben:

$$6\eta_0^2 = (4f + \alpha) + (3\alpha - 6)\eta_0 + \beta(\varepsilon_1 - \varepsilon_2)$$

oder, wenn mit 3 multiplicirt und für $18\eta_0^2 + 12\eta_0 + 2$ sein Werth $2\varepsilon_0^2$ gesetzt wird,

$$3\beta(\varepsilon_1 - \varepsilon_2) = 2\varepsilon_0^2 - A\varepsilon_0 - 4p.$$

Ebenso kommt

$$3\beta(\varepsilon_2 - \varepsilon_0) = 2\varepsilon_1^2 - A\varepsilon_1 - 4p,$$
$$3\beta(\varepsilon_0 - \varepsilon_1) = 2\varepsilon_2^2 - A\varepsilon_2 - 4p,$$

und die Multiplication der drei letzten Gleichungen liefert nach einfachen Reductionen die Formel:

$$(\varepsilon_1 - \varepsilon_2)(\varepsilon_2 - \varepsilon_0)(\varepsilon_0 - \varepsilon_1) = -27p\beta$$

also auch

$$(\eta_1 - \eta_2)(\eta_2 - \eta_0)(\eta_0 - \eta_1) = -p\beta.$$

7. Wir wollen jetzt auch die Gleichung betrachten, welche die der Periode η_0 angehörigen Einheitswurzeln zu Wurzeln hat; sie möge durch

$$x^{\frac{p-1}{3}} + M_1 x^{\frac{p-4}{3}} + \ldots + M_{\frac{p-1}{3}} = 0 \tag{39}$$

oder kurz durch $z = 0$ bezeichnet werden. Da nach Nr. 8 der 6. Vorlesung ihre Coëfficienten auf die Form $a_0\eta_0 + a_1\eta_1 + a_2\eta_2$ gebracht werden können, während a_0, a_1, a_2 ganze Zahlen bedeuten, so werden sie nach Substitution der Werthe der Perioden folgende Gestalt annehmen:

$$\tfrac{1}{3}\left(P + (Q + R\varrho)\sqrt[3]{p\varpi} + (Q + R\varrho^2)\sqrt[3]{p\varpi'}\right)$$

wenn mit P, Q, R ebenfalls ganze reelle Zahlen bezeichnet werden. Denkt man sich die Coëfficienten der Gleichung (39) aber in dieser Weise dargestellt, so ergiebt sich z selbst von der Form:

$$z = \tfrac{1}{3}\left(U + (V + W\varrho)\sqrt[3]{p\varpi} + (V + W\varrho^2)\sqrt[3]{p\varpi'}\right),$$

in welcher U, V, W ganze Functionen von x mit reellen Coëfficienten bedeuten.

Nun ergeben sich aus der Gleichung $z = 0$ die beiden ähnlichen Gleichungen $z' = 0$, $z'' = 0$, deren Wurzeln die, in jeder der beiden andern Perioden enthaltenen Einheitswurzeln sind, dadurch, dass man r in r^g und r^{g^2} successive verwandelt oder die Perioden η_0, η_1, η_2 zweimal hinter einander cyclisch vertauscht, was ihren gefundenen Werthen nach nichts Anderes sagt, als dass man $\sqrt[3]{p\varpi}$ und $\sqrt[3]{p\varpi'}$ successive in $\varrho^2\sqrt[3]{p\varpi}$, $\varrho\sqrt[3]{p\varpi'}$ und dann in $\varrho\sqrt[3]{p\varpi}$, $\varrho^2\sqrt[3]{p\varpi'}$ übergehen lässt. Da hierbei die ganzen Functionen U, V, W unverändert bleiben, so wird erhalten:

$$z'' = \tfrac{1}{3}\left(U + (V + W\varrho)\,\varrho\sqrt[3]{p\varpi} + (V + W\varrho^2)\,\varrho^2\sqrt[3]{p\varpi'}\right)$$

$$z' = \tfrac{1}{3}\left(U + (V + W\varrho)\,\varrho^2\sqrt[3]{p\varpi} + (V + W\varrho^2)\,\varrho\sqrt[3]{p\varpi'}\right).$$

Das Product der drei Functionen z, z', z'', welches der Function $X = \dfrac{x^p - 1}{x - 1}$ gleich ist, kann durch diese Formeln leicht gefunden werden, wenn man die Identität

$$(\alpha+\beta+\gamma)(\alpha+\beta\varrho+\gamma\varrho^2)(\alpha+\beta\varrho^2+\gamma\varrho) = \alpha^3+\beta^3+\gamma^3 - 3\alpha\beta\gamma$$

beachtet. So gelangt man zu folgender interessanten

und der Gleichung (16) entsprechenden Formel:

$$(40)\quad 27 \,.\, \frac{x^p-1}{x-1} = U^3 + Y^3 \,.\, p\varpi + Z^3 \,.\, p\varpi' - 3p \,.\, UYZ,$$

wenn $Y = V + W\varrho$, $Z = V + W\varrho^2$ gesetzt wird, und U, V, W gewisse ganze Functionen von x bezeichnen. Nachdem man auch für ϖ und ϖ' ihre conjugirten Werthe $a + b\varrho$ und $a + b\varrho^2$ gesetzt hat, verschwindet übrigens aus der rechten Seite dieser Gleichung das Imaginäre, wie nothwendig und leicht zu übersehen ist.

8. Zur Bildung der Coëfficienten $M_1, M_2, \ldots M_{\frac{p-1}{3}}$ in der Gleichung (39) bedient man sich am Besten der Newton'schen Formeln, weil die Potenzsummen der Wurzeln, auf denen diese Formeln beruhen, leicht angebbar sind. In der That, da

$$T_1 = \eta_0 + \varrho\eta_1 + \varrho^2\eta_2, \quad T_2 = \eta_0 + \varrho^2\eta_1 + \varrho\eta_2$$

gefunden worden, so wird offenbar, wenn $T_1^{(k)}$, $T_2^{(k)}$ wieder die Bedeutung haben, wie in Nr. 6 der vorigen Vorlesung, und wenn s_k, s_k', s_k'' die Summen der k^{ten} Potenzen derjenigen Einheitswurzeln sind, welche resp. die drei Perioden η_0, η_1, η_2 bilden,

$$T_1^{(k)} = \left[\frac{k}{\varpi}\right]^2 T_1 = s_k + \varrho s_k' + \varrho^2 s_k'', \; T_2^{(k)} = \left[\frac{k}{\varpi}\right] T_2 = s_k + \varrho^2 s_k' + \varrho s_k''$$

sein, während ausserdem die Gleichung $s_k + s_k' + s_k'' = -1$ besteht, vorausgesetzt, dass k eine durch p nicht theilbare Zahl sei, da dann die Summe der k^{ten} Potenzen aller Einheitswurzeln den Werth -1 hat. Aus diesen drei Gleichungen findet man leicht:

$$s_k = \tfrac{1}{3}\left(-1 + \left[\frac{k}{\varpi}\right]^2 . \, T_1 + \left[\frac{k}{\varpi}\right] . \, T_2\right)$$

$$s_k'' = \tfrac{1}{3}\left(-1 + \left[\frac{k}{\varpi}\right]^2 . \, \varrho T_1 + \left[\frac{k}{\varpi}\right] . \, \varrho^2 T_2\right)$$

$$s_k' = \tfrac{1}{3}\left(-1 + \left[\frac{k}{\varpi}\right]^2 . \, \varrho^2 T_1 + \left[\frac{k}{\varpi}\right] . \, \varrho T_2\right).$$

Hier sollen diese Formeln benutzt werden, um den Coëfficienten M_3 zu berechnen, aus dessen Werth mit Leichtigkeit der Ergänzungssatz zum cubischen Reciprocitätsgesetze erhalten werden kann. Man hat bekanntlich

$$(41)\qquad 6M_3 = 3s_1s_2 - s_1^3 - 2s_3,$$

und aus den vorigen Gleichungen ergiebt sich

$$3 s_1 s_2 = \tfrac{9}{27}\Big[1 + \Big[\tfrac{2}{\varpi}\Big] p + \Big[\tfrac{2}{\varpi}\Big]^2 p - T_1\Big(1 + \Big[\tfrac{2}{\varpi}\Big]^2 - \varpi' . \Big[\tfrac{2}{\varpi}\Big]\Big)$$
$$- T_2\Big(1 + \Big[\tfrac{2}{\varpi}\Big] - \varpi . \Big[\tfrac{2}{\varpi}\Big]^2\Big)\Big]$$

$$s_1^3 = \tfrac{1}{27}[-1 + p\varpi + p\varpi' - 6p + 3T_1(1 - \varpi' + p) + 3T_2(1 - \varpi + p)]$$

$$s_3 = \tfrac{9}{27}\Big(-1 + \Big[\tfrac{3}{\varpi}\Big]^2 . T_1 + \Big[\tfrac{3}{\varpi}\Big] . T_2\Big),$$

wenn man bei der Berechnung dieser Ausdrücke auf die Formeln

$$T_1^3 = p\varpi, \quad T_1 T_2 = p, \quad T_2^3 = p\varpi'$$

und die folgenden, daraus unmittelbar hervorgehenden:

$$T_1^2 = \varpi T_2, \quad T_2^2 = \varpi' T_1, \quad T_1^2 T_2 = p T_1, \quad T_1 T_2^2 = p T_2$$

Rücksicht nimmt. Auf diese Weise erhält man für den Coëfficienten von T_2 in dem Ausdrucke (41) folgenden Werth:

$$\tfrac{1}{27}\Big(-12 + 3\varpi - 3p - 9 . \Big[\tfrac{2}{\varpi}\Big] + 9\varpi . \Big[\tfrac{2}{\varpi}\Big]^2 - 18 . \Big[\tfrac{3}{\varpi}\Big]\Big).$$

Da nun M_3 nach Nr. 7 auf die Form

$$\tfrac{1}{3}[P + (Q + R\varrho) T_1 + (Q + R\varrho^2) T_2]$$

gebracht werden kann, so muss der eben gefundene Werth der ganzen complexen Zahl $2(Q + R\varrho^2)$ gleich, und folglich der in der Klammer enthaltene Ausdruck durch 27 theilbar sein. Die so erhaltene Congruenz

$$-4 + \varpi - p - 3 . \Big[\tfrac{2}{\varpi}\Big] + 3\varpi . \Big[\tfrac{2}{\varpi}\Big]^2 - 6 . \Big[\tfrac{3}{\varpi}\Big] \equiv 0 \pmod{9}$$

reducirt sich aber, wenn man bedenkt, dass $\varpi \equiv -1$ und

$$\Big[\tfrac{2}{\varpi}\Big] + \Big[\tfrac{2}{\varpi}\Big]^2 = \varrho^\alpha + \varrho^{2\alpha},$$

also für jeden Fall, den α darbieten kann, congruent $-1 \pmod{3}$ ist, auf folgende:

$$p - \varpi + 1 \equiv 3 . \Big[\tfrac{3}{\varpi}\Big] \pmod{9}$$

oder

$$\tfrac{1}{3}(p - \varpi + 1) \equiv \Big[\tfrac{3}{\varpi}\Big] \pmod{3}.$$

Nun ist $\varpi = a + b\varrho$, $p = a^2 - ab + b^2$; setzt man $a = 3m - 1$, $b = 3n$, so findet man leicht:

$$\tfrac{1}{3}(p - \varpi + 1) \equiv 1 + n(1 - \varrho) \pmod{3}$$

folglich

$$\left[\frac{3}{\varpi}\right] \equiv 1 + n\,(1 - \varrho)\,.$$

Nach den drei Fällen $n \equiv 0, 1, 2$ (mod. 3) wird der Ausdruck zur Rechten dieser Congruenz den Werthen $1,\ 2 - \varrho = 3 + \varrho^2$, $3 - 2\varrho = 3\,(1 - \varrho) + \varrho$ gleich, also den Werthen $1, \varrho^2, \varrho$ oder auch in allen drei Fällen dem Werthe ϱ^{2n} (mod. 3) congruent; also findet man schliesslich die einfache Formel

$$\left[\frac{3}{\varpi}\right] \equiv \varrho^{2n} \pmod{3}$$

oder vielmehr

$$\left[\frac{3}{\varpi}\right] = \varrho^{2n} = \varrho^{\frac{2b}{3}} \tag{42}$$

Es handelt sich aber beim Ergänzungssatze darum, den Werth des Symboles $\left[\frac{1 - \varrho}{\varpi}\right]$ zu bestimmen. Dies geschieht sofort mittels der Identität $(1 - \varrho)^2 = -3\varrho$, welche zuerst

$$\left[\frac{1 - \varrho}{\varpi}\right]^2 = \left[\frac{-3}{\varpi}\right] \cdot \left[\frac{\varrho}{\varpi}\right], \text{ also } \left[\frac{1 - \varrho}{\varpi}\right] = \left[\frac{-3}{\varpi}\right]^2 \cdot \left[\frac{\varrho}{\varpi}\right]^2$$

und dann, mit Rücksicht auf die Gleichungen in Nr. 5 der 14. Vorlesung und auf die soeben erhaltene Beziehung

$$\left[\frac{1 - \varrho}{\varpi}\right] = \varrho^{\frac{4b}{3} + 2\,.\,\frac{p-1}{3}},$$

ergiebt. Da nun b durch 3 theilbar ist, so folgt nach der Gleichung

$$p = (a + b)^2 - 3ab$$

die Congruenz

$$p \equiv (a + b)^2 \text{ also } p - 1 \equiv (a + b + 1)\,(a + b - 1) \pmod{9},$$

und da der zweite Factor der Einheit, der erste der Null (mod. 3) congruent ist,

$$\frac{p - 1}{3} \equiv \frac{a + b + 1}{3} \pmod{3}\,.$$

Hiernach wird $\frac{4b}{3} + 2\,.\,\frac{p - 1}{3} \equiv 2\,.\,\frac{a + 1}{3}$ und folglich

$$\left[\frac{1 - \varrho}{\varpi}\right] = \varrho^{2\,.\,\frac{a+1}{3}}\,.$$

Ist endlich q eine reelle Primzahl von der Form $6n + 5$, so ist nach der Gleichung $(1 - \varrho)^2 = -3\varrho$

$$\left[\frac{1-\varrho}{q}\right]^2 = \left[\frac{-3}{q}\right] \cdot \left[\frac{\varrho}{q}\right],$$

folglich wegen der schon citirten Formeln

$$\left[\frac{1-\varrho}{q}\right] = \varrho^{2 \cdot \frac{q^2-1}{3}},$$

wofür auch, da $\frac{q^2-1}{3} = \frac{q+1}{3}(q-1)$ und $q-1 \equiv 1 \pmod{3}$ ist,

$$\left[\frac{1-\varrho}{q}\right] = \varrho^{2 \cdot \frac{q+1}{3}}$$

geschrieben werden kann. Diese Formel ist offenbar in der, auf den vorigen Fall bezüglichen enthalten, und man gelangt folglich zu dem Satze:

Ist $a + b\varrho$ eine der aus ϱ gebildeten primären complexen Primzahlen, mit Ausnahme der Primzahl $1-\varrho$, so besteht die Gleichung

$$(43) \qquad \left[\frac{1-\varrho}{a+b\varrho}\right] = \varrho^{\frac{2}{3}(a+1)} \text{ *)}.$$

Sechszehnte Vorlesung.

Fortsetzung: Der Fall $p = 4n + 1$.

1. Wir wollen als drittes Beispiel p als eine Primzahl von der Form $4n + 1$ voraussetzen, die vier Perioden $\eta_0, \eta_1, \eta_2, \eta_3$ von $f = \frac{p-1}{4}$ Gliedern bilden, und die Gleichung aufstellen, deren Wurzeln sie sind.**) Wir müssen dabei jedoch von vornherein unterscheiden, ob p die Form $8n + 1$ oder die Form $8n + 5$ habe, und betrachten zunächst jenen ersten

*) Vgl. zu den letzten Nummern dieser Vorlesung die Abhandlungen von Eisenstein „Nachtrag zum cubischen Reciprocitätsgesetz" in Cr. J. Bd. 28 und „über die Formen 3ten Grades mit 3 Variabeln, welche der Kreistheilung ihre Entstehung verdanken" in Cr. J. Bd. 28.

**) Vgl. hierzu Gauss theoria resid. biquadrat. comment. I artt. 15—22.

Fall. In demselben erhält man, da f gerade ist, nach den allgemeinen Kummer'schen Formeln folgende Gleichungen: erstens

$$(1) \qquad \eta_0 + \eta_1 + \eta_2 + \eta_3 = -1;$$

ferner, weil

$$\eta_0\eta_1 + \eta_0\eta_2 + \eta_0\eta_3 + \eta_1\eta_2 + \eta_1\eta_3 + \eta_2\eta_3 = (\eta_0\eta_1 + \eta_1\eta_2 + \eta_2\eta_3 + \eta_3\eta_0) + \tfrac{1}{2}(\eta_0\eta_2 + \eta_1\eta_3 + \eta_2\eta_0 + \eta_3\eta_1)$$

gesetzt werden kann, aus der Formel (7) voriger Vorlesung, wenn successive $k = 1$, $h = 2$ gesetzt wird:

$$(2) \qquad \eta_0\eta_1 + \eta_0\eta_2 + \eta_0\eta_3 + \eta_1\eta_2 + \eta_1\eta_3 + \eta_2\eta_3 = -3 \cdot \frac{f}{2};$$

ferner aus der ersten der Gleichungen (9) ebendaselbst für $k = 1$, $h = 2$:

$$(3) \qquad \eta_0\eta_1\eta_2 + \eta_0\eta_1\eta_3 + \eta_0\eta_2\eta_3 + \eta_1\eta_2\eta_3 = -f^2 + p \cdot m'_2 \cdot$$

Um den letzten Coëfficienten der fraglichen Gleichung, nämlich den Werth von $\eta_0\eta_1\eta_2\eta_3$, zu finden, setzen wir zunächst in der Gleichung (4) ebendaselbst successive $k = 0, 1, 2, 3$ und erhalten mit Rücksicht auf die Gleichungen (10) und (11) folgendes System von Gleichungen:

$$(4) \quad \begin{cases} \eta_0\eta_0 = f + m_0^0\eta_0 + m_1^0\eta_1 + m_2^0\eta_2 + m_3^0\eta_3 \\ \eta_0\eta_1 = \quad m_1^0\eta_0 + m_3^0\eta_1 + m_2'\eta_2 + m_2'\eta_3 \\ \eta_0\eta_2 = \quad m_2^0\eta_0 + m_2'\eta_1 + m_2^0\eta_2 + m_2'\eta_3 \\ \eta_0\eta_3 = \quad m_3^0\eta_0 + m_2'\eta_1 + m_2'\eta_2 + m_1^0\eta_3 \end{cases}$$

sodass das Schema der sechszehn Zahlen:

$$\begin{matrix} m_0^0 & m_1^0 & m_2^0 & m_3^0 \\ m_0' & m_1' & m_2' & m_3' \\ m_0'' & m_1'' & m_2'' & m_3'' \\ m_0''' & m_1''' & m_2''' & m_3''' \end{matrix}$$

auf die fünf Werthe $m_0^0, m_1^0, m_2^0, m_3^0, m_2'$ reducirt ist, zwischen denen nach (6) vor. Vorl. noch folgende Relationen bestehen:

$$(5) \; m_0^0 + m_1^0 + m_2^0 + m_3^0 = f - 1, \; m_1^0 + m_3^0 + 2m_2' = f, \; 2(m_2^0 + m_2') = f.$$

Der dritten der Gleichungen (4) kann man wegen (1) auch die Form geben:

$$\eta_0\eta_2 = (m_2^0 - m_2')(\eta_0 + \eta_2) - m_2',$$

und erhält daraus durch cyclische Vertauschung der Perioden noch die ähnliche Gleichung

$$\eta_1\eta_3 = (m_2^0 - m'_2)(\eta_1 + \eta_3) - m_2',$$

durch deren Multiplication mit der vorigen man findet:

$$\eta_0\eta_1\eta_2\eta_3 = (m_2^0 - m'_2)^2(\eta_0\eta_1 + \eta_1\eta_2 + \eta_2\eta_3 + \eta_3\eta_0) + m'_2(m_2^0 - m'_2) + (m'_2)^2,$$

oder einfacher

$$(6) \qquad \eta_0\eta_1\eta_2\eta_3 = -f\,.\,(m_2^0 - m'_2)^2 + m_2^0 m_2'.$$

2. Um den dritten und letzten Coëfficienten der gesuchten Gleichung vollständig zu bestimmen, müssen wir wieder auf den Zusammenhang der Zahlen m_h^k mit der Function $\psi(h, k, g)$ zurückkommen. Wird nämlich in der Formel (33) der vor. Vorlesung $h = n = \frac{p-1}{4}$ gesetzt, so geht die Function $\psi(h, k, g)$ genau in den Ausdruck

$$\sum_{\mu=1}^{\mu=p-2}\left(g^{\frac{p-1}{4}}\right)^{\text{ind.}(\mu+\mu^2)}$$

über (s. Vorl. 10 Nr. 6), welcher congruent

$$A_0 + A_1 g^{\frac{p-1}{4}} + A_2 g^{2.\frac{p-1}{4}} + A_3 g^{3.\frac{p-1}{4}} \pmod{p}$$

ist, wenn A_0, A_1, A_2, A_3 dieselben Zahlen bezeichnen, wie an der angeführten Stelle, sodass

$$(7) \qquad A_0 + A_1 + A_2 + A_3 = p - 2$$

und $A_0 - A_2 = a$, $A_1 - A_3 = b$ ist. Setzt man andererseits

$$B_0 = \sum_{u,v}{}^0 m_v^u,\quad B_1 = \sum_{u,v}{}' m_v^u,\quad B_2 = \sum_{u,v}{}'' m_v^u,\quad B_3 = \sum_{u,v}{}''' m_v^u$$

und erstreckt diese Summen resp. über alle Werthe u, v aus der Reihe 0, 1, 2, 3, für welche $u + v \equiv 0, 1, 2, 3 \pmod{4}$ wird, so besteht nach (34) der vor. Vorlesung die Gleichung

$$(8) \qquad B_0 + B_1 + B_2 + B_3 = p - 2$$

und nach (33) ebendas. die Congruenz:

$$(9) \qquad B_0 + B_1 g^{\frac{p-1}{4}} + B_2 g^{2.\frac{p-1}{4}} + B_3 g^{3.\frac{p-1}{4}}$$
$$\equiv A_0 + A_1 g^{\frac{p-1}{4}} + A_2 g^{2.\frac{p-1}{4}} + A_3 g^{3.\frac{p-1}{4}} \pmod{p}.$$

Aehnlicherweise findet man, wenn successive $h = n = \frac{p-1}{2}$, $h = n = 3\,.\,\frac{p-1}{4}$ gesetzt wird, wofür $\psi'(h, k, g)$ in die Summen

$$\sum_{\mu=1}^{\mu=p-2}\left(g^{\frac{p-1}{2}}\right)^{\mathrm{ind.}(\mu+\mu^2)} \text{ und } \sum_{\mu=1}^{\mu=p-2}\left(g^{3.\frac{p-1}{4}}\right)^{\mathrm{ind.}(\mu+\mu^2)} \text{ resp.}$$

übergeht, noch folgende Congruenzen:

$$(10)\quad \left.\begin{aligned} & B_0+B_1 g^{3.\frac{p-1}{4}}+B_2 g^{\frac{p-1}{2}}+B_3 g^{\frac{p-1}{4}} \\ & \equiv A_0+A_1 g^{3\frac{p-1}{4}}+A_2 g^{\frac{p-1}{2}}+A_3 g^{\frac{p-1}{4}} \\ & B_0+B_1 g^{\frac{p-1}{2}}+B_2+B_3 g^{\frac{p-1}{2}} \\ & \equiv A_0+A_1 g^{\frac{p-1}{2}}+A_2+A_3 g^{\frac{p-1}{2}} \end{aligned}\right\} \pmod{p},$$

welche in Verbindung mit der vorigen und den Gleichungen (7) und (8) wieder die Identität der Zahlen B_0, B_1, B_2, B_3 mit den Zahlen A_0, A_1, A_2, A_3 resp. beweisen. Man findet daher

$$a=\sum_{u,v}^{0} m_v^u-\sum_{u,v}'' m_v^u, \quad b=\sum_{u,v}' m_v^u-\sum_{u,v}''' m_v^u,$$

oder, ausgeführt geschrieben und mit Rücksicht auf die Eigenschaften der Zahlen m_h^k:

$$(11)\quad \begin{aligned} a &= m_0{}^0+m_2{}^0+2m'_2-2m_2{}^0-m_3{}^0-m_1{}^0 \\ &= m_0{}^0+2m'_2-m_1{}^0-m_2{}^0-m_3{}^0, \end{aligned}$$

$$(12)\quad b=2(m_1{}^0-m_3{}^0).$$

Nunmehr können die Werthe m_h^k berechnet werden. Aus den Gleichungen (5) ergeben sich

$$(13)\quad -m_1{}^0-m_3{}^0=-f+2m'_2=-2m_2{}^0$$

$$(14)\quad m_0{}^0=-m_2{}^0+2m'_2-1,$$

also

$$(15)\quad a=4(m'_2-m_2{}^0)-1.$$

Verbindet man hiermit die dritte der Gleichungen (5), so findet man

$$(16)\quad 8m'_2=2f+a+1, \quad 8m_2{}^0=2f-a-1.$$

Aus (12) und (13) findet man noch

$$4m_1{}^0=4m_2{}^0+b, \quad 4m_3{}^0=4m_2{}^0-b,$$

also nach (16):

$$(17)\quad 8m_1{}^0=2f+2b-a-1, \quad 8m_3{}^0=2f-2b-a-1$$

und endlich aus (14) und (16):

$$(18)\quad 8m_0{}^0=3a+2f-5.$$

Nach diesen Resultaten gelangt man durch Substitution in die Formeln (3) und (6) durch leichte Reductionen zu den Gleichungen

$$\eta_0\eta_1\eta_2 + \eta_0\eta_1\eta_3 + \eta_0\eta_2\eta_3 + \eta_1\eta_2\eta_3 = \frac{p(a+1)+2f}{8}$$

$$\eta_0\eta_1\eta_2\eta_3 = \frac{-p(a+1)^2+4f^2}{64}.$$

Folglich wird die Gleichung vierten Grades, von welcher die Perioden $\eta_0, \eta_1, \eta_2, \eta_3$ Wurzeln sind, folgende Gestalt annehmen:

$$(19) \qquad x^4 + x^3 - 3\cdot\frac{p-1}{8}\cdot x^2 - \frac{p(a+1)+\frac{p-1}{2}}{8}\cdot x - \frac{p(a+1)^2-\left(\frac{p-1}{2}\right)^2}{64} = 0.$$

Dieselbe vereinfacht sich jedoch um ein Bedeutendes, wenn man die Substitution $4x + 1 = y$ macht, wodurch die Gleichung

$$(20) \qquad (y^2 - p)^2 = 4p\,(y + a)^2$$

hervorgeht.

3. Ist zweitens p von der Form $8n+5$, also $f = \frac{p-1}{4}$ ungerade, so müssen die Betrachtungen den Kummer'schen Formeln gemäss etwas modificirt werden. Zwar ist wieder zuerst

$$(21) \qquad \eta_0 + \eta_1 + \eta_2 + \eta_3 = -1,$$

jedoch erhält schon der zweite Coëfficient der gesuchten Gleichung einen andern Werth, nämlich nach Formel (7) der vor. Vorlesung

$$(22) \quad \eta_0\eta_1 + \eta_0\eta_2 + \eta_0\eta_3 + \eta_1\eta_2 + \eta_1\eta_3 + \eta_2\eta_3 = \frac{p-3f}{2} = \frac{p+3}{8}.$$

Die zweite der Gleichungen (9) ebendas. liefert sodann, indem $k = 1$, $h = 2$ gesetzt wird, mit Rücksicht auf die dortigen Gleichungen (10) und (11):

$$(23) \quad \eta_0\eta_1\eta_3 + \eta_0\eta_1\eta_3 + \eta_0\eta_2\eta_3 + \eta_1\eta_2\eta_3 = -f^2 + p\,.\,m'_1.$$

Denselben Formeln zu Folge nimmt hier das System der Gleichungen (4) folgende Gestalt an:

$$(24) \left\{ \begin{aligned} \eta_0\eta_0 &= \quad m_0{}^0\eta_0 + m_1{}^0\eta_1 + m_2{}^0\eta_2 + m_3{}^0\eta_3 \\ \eta_0\eta_1 &= \quad m'_1\eta_0 + m'_1\eta_1 + m_3{}^0\eta_2 + m_1{}^0\eta_3 \\ \eta_0\eta_2 &= f + m_0{}^0\eta_0 + m'_1\eta_1 + m_0{}^0\eta_2 + m'_1\eta_3 \\ \eta_0\eta_3 &= \quad m'_1\eta_0 + m_3{}^0\eta_1 + m_1{}^0\eta_2 + m'_1\eta_3, \end{aligned} \right.$$

während zwischen den Coëfficienten die Beziehungen:

(25) $2(m_0^0 + m'_1) = f - 1, \quad m_0^0 + m_1^0 + m_2^0 + m_3^0 = f,$

$$m_1^0 + m_3^0 + 2m'_1 = f$$

stattfinden. Giebt man der dritten der Gleichungen (24) mittelst (21) die Form

$$\eta_0\eta_2 = f + m_0^0(\eta_0 + \eta_2) + m'_1(\eta_1 + \eta_3) = f - m'_1 + (m_0^0 - m'_1)(\eta_0 + \eta_2)$$

und multiplicirt sie mit der durch cyclische Vertauschung der Perioden daraus entstehenden:

$$\eta_1\eta_3 = f - m'_1 + (m_0^0 - m'_1)(\eta_1 + \eta_3),$$

so ergiebt sich

$$\eta_0\eta_1\eta_2\eta_3 = (m_0^0 - m'_1)^2 \cdot (\eta_0\eta_1 + \eta_1\eta_2 + \eta_2\eta_3 + \eta_3\eta_0)$$
$$- (m_0^0 - m'_1)(f - m'_1) + (f - m'_1)^2,$$

oder, da nach (7) vor. Vorlesung $\eta_0\eta_1 + \eta_1\eta_2 + \eta_2\eta_3 + \eta_3\eta_0 = -f$ gefunden wird,

(26) $\eta_0\eta_1\eta_2\eta_3 = (f - m'_1)^2 - (f - m'_1)(m_0^0 - m'_1) - f(m_1^0 - m'_1)^2.$

Nun ist aber nach den Betrachtungen der vor. Nr., welche auch dem Falle $p = 8n + 5$ sich anpassen,

$$a = \sum_{u,v}^{0} m_v^u - \sum_{u,v}^{''} m_v^u, \quad b = \sum_{u,v}^{'} m_v^u - \sum_{u,v}^{'''} m_v^u,$$

oder vielmehr, da das Schema der 16 Grössen m_v^u hier nach (24) auf 5 verschiedene reducirt ist,

(27) $a = m_0^0 + m_1^0 + m_3^0 - m_2^0 - 2m'_1, \quad b = 2(m_1^0 - m_3^0).$

Um zunächst die Coëfficienten m_h^k zu bestimmen, schliessen wir aus den Gleichungen (25)

(28) $m_1^0 + m_3^0 = f - 2m'_1,$

(29) $-m_2^0 = m_0^0 + m_1^0 + m_3^0 - f = m_0^0 - 2m'_1,$

also $a = 2m_0^0 - 6m'_1 + f$

oder nach der ersten der Gleichungen (25)

(30) $a = 4(m_0^0 - m'_1) + 1.$

Diese Gleichung, mit der eben genannten verbunden, liefert nun sogleich

(31) $8m_0^0 = 2f + a - 3, \quad 8m'_1 = 2f - a - 1;$

ferner kommt aus der Verbindung der beiden Gleichungen (27) und (28)

(32) $8m_1^0 = 2f + 2b + a + 1, \quad 8m_3^0 = 2f - 2b + a + 1,$

endlich aus (29):

(33) $$8 m_2^0 = 2f - 3a + 1.$$

Setzt man nun die gefundenen Werthe in die Gleichungen (23) und (26) ein, so findet man nach leichten Rechnungen

$$8(\eta_0\eta_1\eta_2 + \eta_0\eta_1\eta_3 + \eta_0\eta_2\eta_3 + \eta_1\eta_2\eta_3) = -(a+1)\,p + 2f$$
$$64\,.\,\eta_0\eta_1\eta_2\eta_3 = 4(p-f)^2 - p(a-1)^2.$$

Daher wird die Gleichung, welche die vier Perioden zu Wurzeln hat, in dem Falle einer Primzahl p von der Form $8n+5$ die folgende sein:

(34) $$x^4 + x^3 + \frac{p+3}{8}x^2 + \frac{(a+1)p-2f}{8}\,.\,x + \frac{4(p-f)^2 - p(a-1)^2}{64} = 0.$$

Setzt man jedoch auch hier wieder $4x+1=y$, so gelangt man zu der sehr viel einfacheren Gleichung:

(35) $$(y^2 + 3p)^2 = 4p\,(y-a)^2.$$

Die Vergleichung dieser letztern mit der beim vorigen Falle in (20) erhaltenen gestattet, beide Formeln in eine zusammenzuziehen und nachstehendes Resultat auszusprechen: Bezeichnet man diejenige Zerfällung der Primzahl p von der Form $4n+1$ in die Summe zweier Quadrate, bei welcher die Basis A des ungeraden Quadrates der Eins (mod. 4) congruent ist, durch

$$p = A^2 + B^2,$$

so lässt sich die Gleichung, welcher die aus den vier Perioden von $\frac{p-1}{4}$ Gliedern zusammengesetzten Werthe $1+4\eta_0$, $1+4\eta_1$, $1+4\eta_2$, $1+4\eta_3$ genügen, schreiben wie folgt:

(36) $$\left[y^2 + \left(1 - 2\,.\,(-1)^{\frac{p-1}{4}}\right)p\right]^2 = 4p\,.\,(y-A)^2.$$

Denn, ist $p = 8n+1$, so hat nach Nr. 5 der 10. Vorlesung a die Form $4n-1$, also ist $A = -a$ und $1 - 2(-1)^{\frac{p-1}{4}} = -1$; ist aber $p = 8n+5$, so hat a die Form $4n+1$, also ist $A = +a$, während $1 - 2(-1)^{\frac{p-1}{4}} = +3$ wird. In dieser Gestalt ist die Gleichung zuerst durch Lebesgue dargestellt worden.*)

*) S. Comptes Rendus LI.

4. Die Wurzeln dieser Gleichung oder auch die Perioden können nach den Formeln der 13. Vorlesung sofort angegeben werden. Denn aus den Ausdrücken

$$\eta_0 = \sum_{m=0}^{m=f-1} r^{g^{4m}}, \quad \eta_1 = \sum_{m=0}^{m=f-1} r^{g^{4m+1}}, \quad \eta_2 = \sum_{m=0}^{m=f-1} r^{g^{4m+2}}, \quad \eta_3 = \sum_{m=0}^{m=f-1} r^{g^{4m+3}}$$

ergeben sich die Gleichungen

$$(37)\qquad \begin{cases} \eta_0 + i\eta_1 - \eta_2 - i\eta_3 = S_1 \\ \eta_0 - \eta_1 + \eta_2 - \eta_3 = S_2 \\ \eta_0 - i\eta_1 - \eta_2 + i\eta_3 = S_3\,, \end{cases}$$

und diese bestimmen, mit der Gleichung $\eta_0 + \eta_1 + \eta_2 + \eta_3 = -1$ verbunden, für die Perioden folgende Werthe:

$$\eta_0 = \tfrac{1}{4}(-1 + S_1 + S_2 + S_3), \quad \eta_1 = \tfrac{1}{4}(-1 - i\,.\,S_1 - S_2 + iS_3)$$
$$\eta_2 = \tfrac{1}{4}(-1 - S_1 + S_2 - S_3), \quad \eta_3 = \tfrac{1}{4}(-1 + i\,.\,S_1 - S_2 - iS_3),$$

welche bekannte sind, da die Werthe der Ausdrücke S_1, S_2, S_3 am angeführten Orte gefunden worden sind.

Bezeichnen s_k, s'_k, s''_k, s'''_k resp. die k^{ten} Potenzsummen der in den vier Perioden enthaltenen Wurzeln, so können auch diese leicht gefunden werden, da offenbar, wenn k nicht durch p theilbar ist, folgende Gleichungen bestehen:

$$s_k + s'_k + s''_k + s'''_k = -1$$
$$s_k + is'_k - s''_k - is'''_k = S_1^{(k)} = \left(\left(\frac{k}{\varpi}\right)\right)^3 . S_1$$
$$s_k - s'_k + s''_k - s'''_k = S_2^{(k)} = \left(\left(\frac{k}{\varpi}\right)\right)^2 . S_2$$
$$s_k - is'_k - s''_k + is'''_k = S_3^{(k)} = \left(\left(\frac{k}{\varpi}\right)\right) . S_3,$$

aus denen sich z. B.

$$(38)\qquad s_k = \tfrac{1}{4}\left(-1 + \left(\left(\frac{k}{\varpi}\right)\right)^3 . S_1 + \left(\left(\frac{k}{\varpi}\right)\right)^2 . S_2 + \left(\left(\frac{k}{\varpi}\right)\right) . S_3\right)$$

findet. Mit Hülfe dieser Potenzsummen können sodann die Coëfficienten derjenigen Gleichungen gebildet werden, denen die in je einer der vier Perioden enthaltenen Wurzeln Genüge leisten, und es greifen natürlich hier ganz ähnliche Bemerkungen Platz, als wir bei den Perioden von $\frac{p-1}{2}$ und $\frac{p-1}{3}$ Gliedern zu machen Gelegenheit gehabt haben. Namentlich kann hier der Ausdruck $256X$ in einer biquadratischen Form dargestellt

werden, deren Ableitung wir dem Leser überlassen können, da sie nach dem früher Bemerkten keinerlei Schwierigkeit bietet. Ich begnüge mich deshalb hier damit, die Darstellung einfach anzugeben, sie ist folgende:

$$(39) \qquad 256 \cdot \frac{x^p - 1}{x - 1} = [U^2 + pW^2 - 2ep(V^2 + V'^2)]^2$$
$$- 4p\,[UW - ea(V^2 - V'^2) + 2eb\,VV']^2,$$

wenn unter U, V, V', W gewisse ganze Functionen von x mit reellen ganzen Coëfficienten, und unter e zur Abkürzung die Potenz $(-1)^{\frac{p-1}{4}}$ verstanden wird.

5. Nicht übergehen darf ich jedoch die Anwendung, welche man von den letzten Resultaten machen kann, um noch einen, den biquadratischen Character der Zwei bestimmenden Satz abzuleiten.

Hier muss zunächst eine Vorbemerkung gemacht werden. Versetzen wir uns wieder auf den Boden der reellen Zahlentheorie und nennen g irgend eine primitive Wurzel der Primzahl p von der Form $4n + 1$, so können wir alle Reste (mod. p) in vier Classen A, B, C, D von je $f = \frac{p-1}{4}$ Gliedern vertheilen, welche dadurch characterisirt werden, dass ein Rest m zu A, B, C, D gehören soll, je nachdem der ind. m oder die Zahl μ in der Congruenz $m \equiv g^\mu$ (mod. p) congruent 0, 1, 2, 3 (mod. 4) resp. zu setzen ist. Aus Nr. 1 der 9. Vorlesung folgt, dass die Reste der Classe A, welche den Zahlen $1, g^4, g^8, \ldots\ldots g^{4(f-1)}$ congruent sind, die biquadratischen Reste (mod. p) repräsentiren; alle übrigen sind demnach die biquadratischen Nichtreste. Da jedoch die Reste der beiden Classen A und C zusammengenommen nach derselben Stelle die quadratischen Reste (mod. p) repräsentiren, da sie den Zahlen $1, g^2, g^4, \ldots\ldots g^{p-3}$ congruent sind, so werden die Reste der Classe C diejenigen Zahlen repräsentiren, welche zwar quadratische oder nicht mehr biquadratische Reste sind. Die Zahlen der beiden Classen A und C sind demnach ganz bestimmte; anders verhält es sich mit den Zahlen, welche jede der Classen B, D bilden, denn diese Classen hängen offenbar von der willkürlichen Wahl der primitiven Wurzel g ab und vertauschen sich unter einander bei passender Wahl einer andern primitiven Wurzel.

Nunmehr sei ϖ ein (primärer) Factor von p, und g werde so gewählt, dass $g^{\frac{p-1}{4}} \equiv i \pmod{\varpi}$ ist. Da nach dem Ende der Nr. 5 in der 12. Vorlesung alle durch ϖ nicht theilbaren complexen Zahlen den reellen Zahlen $1, 2, 3, \ldots . p - 1$ oder, was dasselbe sagt, den Potenzen $1, g, g^2, \ldots . g^{p-2} \pmod{\varpi}$ congruent sind, kann man auch hier dieselbe Classificirung aller reellen und complexen Zahlen in die Classen A, B, C, D beibehalten. Dabei ist nun beachtenswerth, dass jede reelle Zahl m stets nach beiden Moduln, p sowohl als ϖ, in dieselbe Classe gehört. In der That: aus der Congruenz $g^\mu \equiv m \pmod{p}$ folgt sofort auch $g^\mu \equiv m \pmod{\varpi}$; aber auch umgekehrt, wenn $m - g^\mu$ durch ϖ theilbar, etwa gleich $\varpi(\alpha + \beta i)$ ist, so ergiebt sich durch Vertauschung von i mit $-i$ auch $m - g^\mu = \varpi'(\alpha - \beta i)$ d. h. $m - g^\mu$ durch ϖ' theilbar und folglich durch $\varpi\varpi' = p$, d. h. $m \equiv g^\mu \pmod{p}$, womit die Behauptung erwiesen ist.

Erhebt man nach dieser Bemerkung die Congruenz $m \equiv g^{4k+\alpha} \pmod{\varpi}$, in welcher α eine der Zahlen 0, 1, 2, 3 bezeichne, zur $\frac{p-1}{4}$ten Potenz, so ergiebt sich $m^{\frac{p-1}{4}} \equiv g^{\alpha . \frac{p-1}{4}} \equiv i^\alpha \pmod{\varpi}$ d. h. $\left(\left(\frac{m}{\varpi}\right)\right) = i^\alpha$. Umgekehrt, besteht diese Gleichung, so muss $m \equiv g^{4k+\alpha} \pmod{\varpi}$ sein; denn, da $m \equiv g^h$ gesetzt werden darf, so muss $m^{\frac{p-1}{4}} \equiv g^{h . \frac{p-1}{4}} \equiv i^\alpha$ sein, was wegen $g^{\frac{p-1}{4}} \equiv i$ nur möglich ist, wenn $h \equiv \alpha \pmod{4}$ oder von der Form $4k + \alpha$ ist. Hieraus ergiebt sich offenbar, dass eine reelle Zahl m zu den Classen $A, B, C, D \pmod{\varpi}$ oder $\pmod{p}$ gehört, jenachdem das Zeichen $\left(\left(\frac{m}{\varpi}\right)\right)$ die Werthe $1, i, i^2, i^3$ resp. besitzt.

6. Nach dieser allgemeinen Vorbemerkung untersuchen wir nun, zu welcher der vier Classen die Zwei in Bezug auf einen Primzahlmodulus p von der Form $4n + 1$ gehört. Dabei müssen wir zunächst wieder die beiden Fälle, welche die Primzahl p darbieten kann, getrennt behandeln.

Sei also zuerst p von der Form $8n + 1$. Entwickelt man den Ausdruck

$$M = s_1^2 - s_2 = \left(\sum_{m=0}^{m=f-1} r^{g^{4m}}\right)^2 - \sum_{m=0}^{m=f-1} r^{2g^{4m}}$$

nach den Potenzen von r, so müssen nach dem binomischen Satze alle Coëfficienten durch Zwei theilbar sein. Nun ist nach (38):

$$s_2 = \tfrac{1}{4}(-1 + \varepsilon^3 . S_1 + \varepsilon^2 . S_2 + \varepsilon . S_3)$$

wenn zur Abkürzung $\varepsilon = \left(\left(\frac{2}{\varpi}\right)\right)$ gesetzt wird, oder, wenn man nach (37) S_1, S_2, S_3 durch die Perioden ausdrückt,

$$(40)\quad 16 s_2 = 4[-1 + \varepsilon^3(\eta_0 + i\eta_1 - \eta_2 - i\eta_3) + \varepsilon^2(\eta_0 - \eta_1 + \eta_2 - \eta_3) \\ + \varepsilon(\eta_0 - i\eta_1 - \eta_2 + i\eta_3)].$$

Andererseits kann man $s_1^2 = \eta_0^2$ nach der ersten der Gleichungen (4) bestimmen und erhält, wenn für die Coëfficienten m_h^k ihre Werthe gesetzt werden,

$$16 s_1^2 = 16f + \eta_0(6a + 4f - 10) + \eta_1(4b + 4f - 2a - 2) \\ + \eta_2(4f - 2a - 2) + \eta_3(4f - 4b - 2a - 2).$$

Hieraus ergiebt sich, indem man die Gleichung (1) benutzt, die constanten Theile durch die Perioden auszudrücken, und vermittelst der Beziehung $4f + 1 = p$ folgender Werth der Differenz:

$$16(s_1^2 - s_2) = \eta_0(6a - 3p - 11 - 4\varepsilon - 4\varepsilon^2 - 4\varepsilon^3) \\ + \eta_1(4b - 2a - 3p - 3 + 4i\varepsilon + 4\varepsilon^2 - 4i\varepsilon^3) \\ + \eta_2(-2a - 3p - 3 + 4\varepsilon - 4\varepsilon^2 + 4\varepsilon^3) \\ + \eta_3(-4b - 2a - 3p - 3 - 4i\varepsilon + 4\varepsilon^2 + 4i\varepsilon^3).$$

In diesem Ausdrucke müssen sämmtliche Coëfficienten durch 32 theilbar sein, dasselbe also auch von der Differenz zweier Coëfficienten z. B. des zweiten und dritten gelten und so nachstehende Congruenz hervorgehen:

$$4b - 4(1 + i)\varepsilon^3 + 8\varepsilon^2 - 4(1 - i)\varepsilon \equiv 0 \pmod{32}$$

also

$$(41)\quad b - (1 + i)\varepsilon^3 + 2\varepsilon^2 - (1 - i)\varepsilon \equiv 0 \pmod{8}.$$

Es muss nun bemerkt werden, dass man von vornherein für $\varepsilon = \left(\left(\frac{2}{\varpi}\right)\right)$ die Werthe $\pm i$ auszuschliessen hat. In der That, aus dem Satze in Nr. 3 der vorigen Vorlesung wissen wir, dass die Zwei in der reellen Theorie von jeder Primzahl p von der Form $8n + 1$ quadratischer Rest ist, demnach entweder zur Classe A oder zur Classe C gehört; es ist also $\left(\left(\frac{2}{\varpi}\right)\right)$ entweder $+1$ oder -1. Hiernach lehrt aber die Congruenz (41), dass

wenn $\varepsilon = \left(\left(\frac{2}{\varpi}\right)\right) = +1$ ist, $b \equiv 0 \pmod{8}$ also $\frac{b}{2} \equiv 0 \pmod{4}$,

wenn $\varepsilon = \left(\left(\frac{2}{\varpi}\right)\right) = -1$ ist, $b \equiv 4 \pmod{8}$ also $\frac{b}{2} \equiv 2 \pmod{4}$

sein muss. —

Zweitens sei p von der Form $8n + 5$. Alsdann muss $s_1^2 = \eta_0^2$ nach der ersten der Gleichungen (24) bestimmt werden und nimmt, wenn für die Coëfficienten ihre in Nr. 3 gefundenen Werthe substituirt werden, folgende Form an:

$$16 s_1^2 = (4f + 2a - 6)\eta_0 + (4f + 4b + 2a + 2)\eta_1 + (4f - 6a + 2)\eta_2 + (4f - 4b + 2a + 2)\eta_3,$$

also erhält man in diesem Falle

$$\begin{aligned} 16(s_1^2 - s_2) = {} & \eta_0 (p + 2a - 11 - 4\varepsilon - 4\varepsilon^2 - 4\varepsilon^3) \\ & + \eta_1 (p + 4b + 2a - 3 + 4i\varepsilon + 4\varepsilon^2 - 4i\varepsilon^3) \\ & + \eta_2 (p - 6a - 3 + 4\varepsilon - 4\varepsilon^2 + 4\varepsilon^3) \\ & + \eta_3 (p - 4b + 2a - 3 - 4i\varepsilon + 4\varepsilon^2 + 4i\varepsilon^3) \end{aligned}$$

und aus der Differenz des zweiten und ersten Coëfficienten nachstehende Congruenz:

$$4b + 8 + 4(1 + i)\varepsilon + 8\varepsilon^2 + 4(1 - i)\varepsilon^3 \equiv 0 \pmod{32},$$

also

$$b + 2 + (1 + i)\varepsilon + 2\varepsilon^2 + (1 - i)\varepsilon^3 \equiv 0 \pmod{8}.$$

Da in diesem Falle 2 quadratischer Nichtrest von p ist, so gehört es zu einer der beiden Classen B oder D, und folglich kann $\varepsilon = \left(\left(\frac{2}{\varpi}\right)\right)$ nur einen der Werthe $+i$ oder $-i$ haben. Man findet aber:

wenn $\varepsilon = \left(\left(\frac{2}{\varpi}\right)\right) = +i$ ist, $b \equiv 2 \pmod{8}$ also $\frac{b}{2} \equiv 1 \pmod{4}$,

wenn $\varepsilon = \left(\left(\frac{2}{\varpi}\right)\right) = -i$ ist, $b \equiv 6 \pmod{8}$ also $\frac{b}{2} \equiv 3 \pmod{4}$.

Durch Zusammenfassen der für beide Fälle erhaltenen Resultate gelangen wir zu folgendem, zuerst von Gauss in comment. I theoriae resid. biquadrat. ausgesprochenen und bewiesenen Satze von grosser Eleganz: Ist p eine Primzahl von der Form $4n + 1$ und $p = a^2 + b^2$ diejenige Zerlegung derselben in die Summe zweier Quadrate, welche nach der in Nr. 7 der 10. Vorlesung gelehrten Methode gefunden

wird, so gehört die Zwei zu den Classen A, B, C, D resp., jenachdem $\frac{b}{2} \equiv 0, 1, 2, 3 \pmod{4}$ ist.

Einen sehr einfachen, rein arithmetischen Beweis dieses Satzes findet man in einem Briefe Dirichlet's an Stern, welcher im Cr. J. Bd. 57 pag. 187 abgedruckt ist.

Hier ist der Ort, eine Bemerkung von Stern zu reproduciren, auf welche bereits am Schlusse der 10. Vorlesung hingewiesen worden ist, und die sich auf den Fall einer Primzahl p von der Form $8n+5$ bezieht. Für eine solche finden, wie leicht zu sehen, folgende Congruenzen statt:

$$\left.\begin{array}{l} 2^n \,.\, 1 \,.\, 2 \,.\, 3 \,\ldots\, n \equiv 2 \,.\, 4 \,.\, 6 \,\ldots\, 2n \\ \text{und} \\ 2^{n+1} \,.\, (4n+3)(4n+4) \ldots (5n+3) \equiv 1 \,.\, 3 \,.\, 5 \ldots (2n+1) \end{array}\right\} \pmod{p},$$

da

$$2\,(4n+3) \equiv 1,\ 2\,(4n+4) \equiv 3, \ldots\ 2\,(5n+3) \equiv 2n+1$$

ist. Also kommt auch wegen der Congruenzen:

$$4n+3 \equiv -(4n+2),\ 4n+4 \equiv -(4n+1), \ldots 5n+3 \equiv -(3n+2),$$

und da die Anzahl der Factoren gleich $n+1$ ist,

$$2^{n+1} \,.\, (4n+2)(4n+1) \ldots (3n+2) \equiv (-1)^{n+1} \,.\, 1 \,.\, 3 \,.\, 5 \ldots (2n+1).$$

Durch Verbindung dieser Congruenz mit der ersten findet man sodann

$$2^{2n+1} \,.\, (4n+2)(4n+1) \ldots (3n+2) \equiv (-1)^{n+1} \,.\, \frac{1 \,.\, 2 \,.\, 3 \ldots (2n+1)}{1 \,.\, 2 \,.\, 3 \ldots n}$$

also

$$(42) \quad 2^{2n+1} \equiv (-1)^{n+1} \,.\, \frac{(2n+1)\, 2n \ \ldots (n+1)}{(4n+2)\,(4n+1) \ldots (3n+2)} \pmod{p}\,.$$

Nun wollen wir uns erinnern, dass das Vorzeichen von b mit der Wahl der primitiven Wurzel g wechselt, also erst dann bestimmt angegeben werden kann, wenn diese willkürlich festgestellt worden ist. Nach dem Gaussischen Satze gehört aber in dem hier vorliegenden Falle die Zwei zu einer der beiden Classen B, D, welche mit der Wahl der primitiven Wurzel in gleicher Weise wechseln, wie das Vorzeichen von b; je nach der Wahl von g ist entweder $2 \equiv g^{4k+1}$ oder $2 \equiv g^{4k+3} \pmod{p}$, und im ersten Falle $b \equiv 2$, im zweiten $b \equiv 6 \pmod{8}$. Wenn wir daher übereinkommen, g so zu wählen, dass $2 \equiv g^{4k+1} \pmod{p}$ wird, so muss $b \equiv 2 \pmod{8}$ und das Vorzeichen von b ein durch diese Congruenz völlig bestimmtes werden.

Endlich ist in der 10. Vorlesung gefunden worden:

$$a + b \cdot g^{\frac{p-1}{4}} \equiv 0 \text{ d. i. } b \equiv a \cdot g^{\frac{p-1}{4}} \pmod{p}$$

und

$$a \equiv \tfrac{1}{2} \cdot \frac{1 \cdot 2 \cdot 3 \ldots (4n+2)}{[1 \cdot 2 \cdot 3 \ldots (2n+1)]^2} \equiv \tfrac{1}{2} \cdot \frac{(4n+2)(4n+1) \ldots (2n+2)}{1 \cdot 2 \cdot 3 \ldots (2n+1)}.$$

Da sich nun bei der gewählten primitiven Wurzel $2^{2n+1} \equiv g^{2n+1}$ ergiebt, findet man aus der Verbindung der letzten Congruenzen mit der Congruenz (42):

$$(43) \quad 2b \equiv (-1)^{n+1} \cdot \frac{(2n+2)(2n+3) \ldots (3n+1)}{1 \cdot 2 \cdot 3 \ldots n} \pmod{p}.$$

Das so erhaltene Resultat spricht der Satz aus: **Bestimmt man b als die absolut kleinste Zahl, welche die Congruenz (43) befriedigt, so wird diese Zahl congruent 2 (mod. 8), also positiv oder negativ sein, jenachdem sie, abgesehen vom Vorzeichen, von der Form $8m+2$ oder von der Form $8m+6$ ist.** Man findet z. B. $b = 2$, wenn p eine der Primzahlen 13, 29 bedeutet, aber $b = -6$, wenn $p = 37$ gesetzt wird. —

Siebenzehnte Vorlesung.

Die Periodencongruenzen.

1. In den vorigen Abschnitten sind die wichtigsten Anwendungen, welche man von den Eigenschaften der Resolvante der Kreistheilungsgleichung auf die höhere Arithmetik gemacht hat, und die sich sämmtlich auf die Lehre von den Potenzresten sowie auf die damit eng verbundenen Zerlegungen der Zahlen in Quadrate bezogen, zusammengestellt worden.

Geht man nun über die biquadratischen Reste zu den Potenzresten höheren Grades hinaus, so werden zum Theil ganz neue Betrachtungen nothwendig. Dabei bleibt jedoch der Umstand bestehen, dass ebenso, wie der Untersuchung der biquadratischen und cubischen Reste die complexen Zahlen von den Formen $a + bi$ und $a + b\varrho$ resp. zu Grunde gelegt werden mussten, man sich auch hier in dem Gebiete gewisser complexer Zahlen zu bewegen hat, nämlich solcher, welche aus Einheitswurzeln höherer Grade

zusammengesetzt sind. Die Theorie dieser complexen Zahlen ist ausführlich von Kummer untersucht und zur Erforschung der höheren Reciprocitätsgesetze angewendet worden*). Dem Plane dieses Buches liegt es fern, seine Untersuchungen, welche für sich allein ein Ganzes bilden, vollständig mitzutheilen, es muss vielmehr hier auf dieselben verwiesen werden, welche zudem so vollständig ausgeführt sind, dass kaum etwas Anderes möglich sein würde, als sie abzudrucken. Nur von der ersten Abhandlung Kummer's über die aus Wurzeln der Einheit gebildeten complexen Zahlen soll hier soviel beigebracht werden, als nothwendig ist, um zur Erkenntniss der wahren Natur der Resolvante zu gelangen, und so die vollkommene Wechselbeziehung, welche zwischen der Kreistheilung und der höheren Arithmetik besteht, in das hellste Licht zu setzen.

Die Theorie der zu betrachtenden complexen Zahlen basirt durchaus auf der Auffassung der Gleichungen, welche die e Perioden von f Gliedern zu Wurzeln haben, als Congruenzen in Beziehung auf einen gegebenen Primzahlmodulus; daher soll im Voraus diese Vorlesung der Betrachtung solcher Congruenzen gewidmet sein.

Sind $\eta_0, \eta_1, \ldots . \eta_{e-1}$ die e f-gliedrigen Perioden, so leisten dieselben nach Nr. 7 der 6. Vorlesung einer Gleichung $F(x) = 0$ des e^{ten} Grades Genüge, deren Coëfficienten ganze reelle Zahlen sind. Die zu untersuchende Congruenz ist also folgende:

$$F(x) \equiv 0 \pmod{q}, \tag{1}$$

worin der Modulus eine Primzahl sein soll. Es fragt sich vor Allem, hat diese Congruenz für ein gegebenes q reelle Wurzeln, und wieviele? Da man die Function $F(x)$, wenn x eine unbestimmte ganze Zahl bezeichnet, als gemeinsame Form aller durch sie darstellbaren Zahlen auffassen kann, so lässt sich unsere Frage auch so aussprechen: welche Divisoren hat die

---

*) Die betreffenden Untersuchungen von Kummer befinden sich theils im Crelle'schen Journal, theils in den Abhandlungen und Monatsberichten der Berliner Academie, die hauptsächlichsten Arbeiten in den Bdd. 30, 35, 40 des Journals und in den Jahrgg. 1856, 1857, 1859, 1861 der Abhandlungen. S. auch Liouv. J. Bd. 16 in dem „mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers" eine Zusammenstellung der erstgenannten.

Form $F(x)$? In der letztern Gestalt hat Kummer die Aufgabe in Cr. J. Bd. 30 aufgestellt.

Zur Lösung dieser Frage müssen wir Congruenzen in Anwendung bringen, welche ausser ganzen Zahlen auch die Perioden enthalten; es wird nothwendig sein, zunächst eine Definition zu geben, in welchem Sinne solche Congruenzen zu verstehen sind. Wir bemerken deshalb Folgendes: Bekanntlich kann jede ganze Function der Perioden mit ganzzahligen Coëfficienten auf die Normalform

$$a_0\eta_0 + a_1\eta_1 + \cdots + a_{e-1}\eta_{e-1}$$

gebracht werden, worin die Coëfficienten a ganze Zahlen sind. Zwei solcher Functionen werden nun (mod. q) congruent genannt werden, wenn in den auf die Normalform reducirten Functionen die Coëfficienten gleicher Perioden (mod. q) congruente Zahlen sind. Hiernach werden die so definirten Congruenzen denselben Gesetzen gehorchen, wie die gewöhnlichen oder wie die in der 4. Vorlesung zur Anwendung gebrachten Congruenzen.

2. Nach diesen Vorbemerkungen gehen wir nun aus von der für jedes x giltigen Congruenz (9) in Nr. 8 der 4. Vorlesung:

$$x^{q-1} - 1 \equiv (x-1)(x-2)(x-3)\cdots(x-q+1) \pmod{q},$$

wo wir nur q statt p gesetzt haben. Multiplicirt man dieselbe mit x, so erhält man die folgende:

$$x^q - x \equiv x(x-1)(x-2)\cdots(x-q+1).$$

Da sie identisch ist, also nur aussagt, dass die eine Seite der andern gleich ist, wenn man eine gewisse ganze Function vernachlässigt, deren Coëfficienten sämmtlich durch q theilbar sind, so darf man x durch $y - \eta_h$ ersetzen und findet dann:

$$(2)\quad (y-\eta_h)(y-1-\eta_h)(y-2-\eta_h)\cdots(y-q+1-\eta_h) \equiv (y-\eta_h)^q - (y-\eta_h) \pmod{q}.$$

Nach dem binomischen Lehrsatze ist aber

$$(y-\eta_h)^q \equiv y^q - \eta_h{}^q \pmod{q},$$

also, sobald y eine ganze Zahl bedeutet, nach Fermat's Satze

$$(3)\quad (y-\eta_h)^q \equiv y - \eta_h{}^q \pmod{q}.$$

Nun ist

$$\eta_h = r^{g^h} + r^{g^{e+h}} + \cdots + r^{g^{(f-1)e+h}}.$$

Erhebt man diesen Ausdruck zur q^{ten} Potenz, und vernachlässigt wieder alle durch q theilbaren Glieder, so findet man:

$$\eta_h{}^q \equiv r^{qg^h} + r^{qg^{e+h}} + \ldots . + r^{qg^{(f-1)e+h}} \pmod{p}$$

d. h. wenn $q = p$ ist,

(4) $$\eta_h{}^p \equiv f \pmod{p}$$

folglich nach (3):

(5) $$(y - \eta_h)^p \equiv y - f \pmod{p};$$

ist aber q nicht gleich p, so kann man setzen $q \equiv g^k \pmod{p}$, und dann wird

(6) $$\eta_h{}^q \equiv \eta_{h+k} \pmod{q}$$

also nach (3):

(7) $$(y - \eta_h)^q \equiv y - \eta_{h+k} \pmod{q}.$$

Andererseits ist

$$F(x) = (x - \eta_0)(x - \eta_1) \ldots . (x - \eta_{e-1}).$$

Wenn man daher in (5) für h successive $0, 1, 2, \ldots . e - 1$ substituirt und die so entstehenden Congruenzen sämmtlich in einander multiplicirt, so ergiebt sich offenbar als Resultat:

(8) $$F(y)^p \equiv (y - f)^e \pmod{p},$$

welche Congruenz zeigt, dass die Congruenz $F(y) \equiv 0 \pmod{p}$ nur eine reelle Wurzel, nämlich $y \equiv f$ besitzt.

3. Wird auf dieselbe Weise mit (2) verfahren, wenn q nicht gleich p ist, so findet man, da die rechte Seite nach (7) den Werth $\eta_h - \eta_{h+k}$ annimmt,

(9) $$F(y).F(y-1)\ldots.F(y-q+1) \equiv (\eta_0 - \eta_k)(\eta_1 - \eta_{k+1})\ldots.(\eta_{e-1} - \eta_{k-1}) \pmod{q}.$$

Hierin ist die rechte Seite eine ganze und ganzzahlige Function einer Wurzel der Kreistheilungsgleichung und offenbar unveränderlich bei der Substitution von r^g statt r, also nach der 6. Vorlesung Nr. 6, 2) eine ganze Zahl, welche P heisse. Andererseits bilden die q auf einander folgenden ganzen Zahlen y, $y - 1$, $y - 2, \ldots . y - q + 1$ ein Restensystem (mod. q); hätte also die Congruenz (1) eine Wurzel, so würde ein Factor der linken Seite von (9) durch q theilbar, daher auch die ganze Zahl P, und umgekekrt. Man gelangt so zu dem Satze:

Die nothwendige und hinreichende Bedingung für

die Existenz einer reellen Wurzel der Congruenz (1) ist die Congruenz

$$(10) \qquad P \equiv 0 \pmod{q}.$$

Betrachten wir nun besonders den Fall, in welchem q eine zum Exponenten f (mod. p) gehörige Primzahl bedeutet; da alsdann in der Congruenz $q \equiv g^k$ (mod. p), welche wir angenommen haben, $k =$ ind. q ist, so wird k nach Nr. 10, 3) der 4. Vorlesung durch e theilbar sein. In diesem Falle und allgemeiner, wenn q ein e^{ter} Potenzrest ist, wird aber $\eta_{k+h} = \eta_h$ also die Congruenz (2) mit Rücksicht auf (3) und (6) folgende einfache Gestalt erhalten:

$$(11) \quad (y - \eta_h)(y - 1 - \eta_h) \ldots . (y - q + 1 - \eta_h) \equiv 0 \pmod{q},$$

woraus, wenn $h = 0, 1, 2, \ldots . e - 1$ gesetzt und das Product der entstehenden Congruenzen gebildet wird,

$$F(y) \,.\, F(y-1) \,.\, F(y-2) \ldots . F(y - q + 1) \equiv 0 \pmod{q^e}$$

hervorgeht. Da nun die e Factoren q sich auf die Factoren der linken Seite dieser Congruenz vertheilen müssen, werden im Allgemeinen e Factoren durch q theilbar sein; freilich kann auch der besondere Fall eintreten, dass weniger als e Factoren, dafür aber einzelne mehrfach durch q theilbar sind. Es giebt daher e, gleiche oder verschiedene, Zahlen eines Restsystems, welche die Congruenz $F(x) \equiv 0$ (mod. q) erfüllen. Dieses für das Folgende äusserst wichtige Resultat wollen wir in dem Satze aussprechen:

Die Congruenz (1) besitzt, wenn q eine Primzahl bedeutet, welche e^{ter} Potenzrest von p ist, immer e reelle Wurzeln, welche jedoch nicht nothwendig von einander verschieden zu sein brauchen.

4. Setzt man z. B. $e = p - 1$ also $f = 1$, für welchen Werth des e die Perioden eingliedrig d. h. den Wurzeln der Kreistheilungsgleichung gleich werden, also $F(x)$ in $\frac{x^p - 1}{x - 1}$ übergeht, so findet man den speciellen Satz:

Die Congruenz

$$x^{p-1} + x^{p-2} + \ldots . + x + 1 \equiv 0 \pmod{q}$$

hat $p - 1$ reelle Wurzeln, wenn die Primzahl $q \equiv 1$ (mod. p) d. h. von der Form $2mp + 1$ ist.

Da für diesen Fall

$$P = \left(r - r^{g^k}\right)\left(r^g - r^{g^{k+1}}\right)\left(r^{g^2} - r^{g^{k+2}}\right)\ldots\left(r^{g^{p-2}} - r^{g^{k+p-2}}\right)$$
$$= r^{1+g+g^2+\ldots+g^{p-2}}.\left(1 - r^{g^k-1}\right)\left(1 - r^{g(g^k-1)}\right)\ldots\left(1 - r^{g^{p-2}(g^k-1)}\right)$$

ist, und, sobald nicht $g^k \equiv 1$ (mod. p) d. h. $k \equiv 0$ mod. $(p-1)$ ist, r^{g^k-1} eine Wurzel der Kreistheilungsgleichung ist, folglich

$$\left(1 - r^{g^k-1}\right)\left(1 - r^{g(g^k-1)}\right)\ldots\left(1 - r^{g^{p-2}(g^k-1)}\right) = \left(\frac{x^p-1}{x-1}\right)_{\text{für } x=1} = p$$

gefunden wird, während

$$1 + g + g^2 + \ldots + g^{p-2} = \frac{g^{p-1}-1}{g-1} \equiv 0\ (\text{mod.}\, p),$$

also

$$r^{1+g+g^2+\ldots+g^{p-2}} = 1$$

ist, so ergiebt sich $P = p$, und nach dem ersten Satze der vorigen Nummer das Resultat: Die Form

$$x^{p-1} + x^{p-2} + \ldots + x + 1$$

hat ausser den Primzahldivisoren von der Form $2mp+1$ nur noch den einen Primzahltheiler p.

Ein ähnlicher Satz existirt für den Fall $e = \frac{p-1}{2}$, wo es sich um die zweigliedrigen Perioden

$$r + r^{g^{\frac{p-1}{2}}} = r + r^{-1},\ r^g + r^{g^{\frac{p+1}{2}}} = r^g + r^{-g},\ \ldots\ r^{g^{\frac{p-3}{2}}} + r^{-g^{\frac{p-3}{2}}}$$

handelt, deren Werthe in Nr. 11 der 6. Vorlesung gleich

$$2\cos\frac{2\pi}{p},\ 2\cos\frac{2g\pi}{p},\ \ldots\ 2\cos\frac{2g^{\frac{p-3}{2}}.\pi}{p}$$

gefunden worden sind. Die Gleichung, deren Wurzeln diese Perioden sind, ergiebt sich sogleich aus der Gleichung (3) in Nr. 4 der 1. Vorlesung, wenn man $m = e = \frac{p-1}{2}$ setzt, welche so folgende Gestalt annimmt:

$$F(x) = x^e + x^{e-1} - \frac{e-1}{1}x^{e-2} - \frac{e-2}{1}x^{e-3}$$
$$+ \frac{(e-2)(e-3)}{1.2}x^{e-4} + \ldots = 0.$$

Nach dem zweiten der Sätze voriger Nummer hat diese Gleichung, als Congruenz (mod. q) aufgefasst, für den Fall, dass die Primzahl q ein $\frac{p-1}{2}$ ter Potenzrest von p ist, stets $\frac{p-1}{2}$ reelle

Wurzeln. Jede solche Primzahl leistet der Congruenz $q \equiv g^{k.\frac{p-1}{2}}$ (mod. p), folglich $q^2 \equiv 1$ (mod. p) Genüge, ist also von einer der beiden Formen $2mp + 1$ oder $2mp - 1$.

Andererseits ist

$$\eta_h - \eta_{h+k} = r^{g^h} + r^{-g^h} - r^{g^{h+k}} - r^{-g^{h+k}};$$

welcher Differenz man leicht nachstehende Form giebt:

$$\eta_h - \eta_{h+k} = r^{g^h}\left(1 - r^{g^h(g^k-1)}\right)\left(1 - r^{-g^h(g^k+1)}\right).$$

Da ferner

$$\eta_{h+\frac{p-1}{2}} - \eta_{h+\frac{p-1}{2}+k} = \eta_h - \eta_{k+h}$$

ist, so kann man auch schreiben:

$$P^2 = (\eta_0 - \eta_k)(\eta_1 - \eta_{k+1}) \ldots\ldots (\eta_{p-2} - \eta_{k+p-2}).$$

Setzt man also den obigen Werth von $\eta_h - \eta_{h+k}$ in dies Product ein, so findet man:

$$P^2 = \prod_{h=0}^{h=p-2}\left(1 - r^{g^h(g^k-1)}\right).\prod_{h=0}^{h=p-2}\left(1 - r^{-g^h(g^k+1)}\right).$$

Jedes der Producte hat nun aber den Werth p, wenn weder $g^k \equiv +1$ noch $g^k \equiv -1$ ist, d. h. sobald q, welches congruent g^k gesetzt worden, zu keiner der vorher bereits behandelten Gattungen von Primzahlen gehört. Dann findet sich also $P^2 = p^2$ oder $P = \pm p$, und daraus in Verbindung mit dem ersten der obigen Sätze folgendes Resultat:

Die Form

$$x^e + x^{e-1} - \frac{e-1}{1}x^{e-2} - \frac{e-2}{1}x^{e-3} + \frac{(e-2)(e-3)}{1.2}x^{e-4} + \ldots.$$

hat ausser den Primzahltheilern von den Formen $2mp \pm 1$ nur den einzigen Primzahltheiler p.

Setzt man endlich $e = 2$, $f = \frac{p-1}{2}$, so nimmt die Congruenz (1) die Form an:

$$(12) \qquad x^2 + x + \frac{1 - (-1)^{\frac{p-1}{2}}.p}{4} \equiv 0 \text{ (mod. } q),$$

welche durch die Substitution $2x + 1 = y$ in die folgende:

$$(13) \qquad y^2 \equiv (-1)^{\frac{p-1}{2}}.p \text{ (mod. } q)$$

übergeht. Es ist offenbar, dass diese gleichzeitig mit jener statt-

findet oder nicht stattfindet; denn, wenn die erstere durch einen Werth von x befriedigt wird, so erhält man eine Wurzel der zweiten durch die Congruenz $y \equiv 2x + 1 \pmod{q}$; aber auch umgekehrt schliesst man aus dem Bestehen der letztern das Stattfinden der erstern, da man die Wurzel y der Congruenz (13) stets als ungerade voraussetzen darf, indem auch $y + q$ eine Wurzel und eine der Zahlen $y, y + q$ ungerade ist. Jenachdem nun aber die Congruenz (13) statt hat oder nicht, ist $(-1)^{\frac{p-1}{2}} . p$ quadratischer Rest von q, also nach dem **Euler**'schen Criterium (s. Vorl. 9, Nr. 2)

$$(-1)^{\frac{p-1}{2}.\frac{q-1}{2}} . p^{\frac{q-1}{2}} \equiv 1 \pmod{q} \text{ d. h. } (-1)^{\frac{p-1}{2}.\frac{q-1}{2}} . \left(\frac{p}{q}\right) = +1,$$

oder quadratischer Nichtrest also

$$(-1)^{\frac{p-1}{2}.\frac{q-1}{2}} . p^{\frac{q-1}{2}} \equiv -1 \pmod{q} \text{ d. h. } (-1)^{\frac{p-1}{2}.\frac{q-1}{2}} . \left(\frac{p}{q}\right) = -1.$$

Nach dem ersten Satze der vorigen Nummer können dieselben Bedingungen aber auch noch anders ausgesprochen werden; da nämlich hier

$$P \equiv (\eta_0 - \eta_k)(\eta_1 - \eta_{k+1}) \pmod{q}$$

durch q theilbar wird, wenn k eine gerade Zahl, also q quadratischer Rest von p, $\left(\frac{q}{p}\right) = +1$ ist, dagegen

$$P \equiv -(\eta_0 - \eta_1)^2 \equiv -(-1)^{\frac{p-1}{2}} . p,$$

also nicht durch q theilbar wird, wenn k ungerade, d. h. q quadratischer Nichtrest von p, $\left(\frac{q}{p}\right) = -1$ ist, so findet je nach diesen beiden Fällen die Congruenz (12) statt oder nicht. Die Vergleichung dieses Resultates mit dem vorigen liefert aber in allen Fällen die Gleichung

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}} . \left(\frac{p}{q}\right)$$

d. h. einen neuen Beweis des **Legendre**'schen **Reciprocitätsgesetzes**.*)

5. Es bezeichne nun q eine zum Exponenten $f \pmod{p}$

---

*) Vgl. Lebesgue in den Comptes Rendus LI, pag. 9.

gehörige Primzahl und $a_1, a_2, \ldots a_\alpha$ seien die verschiedenen Wurzeln der Congruenz (1), sodass $\alpha = e$ oder $\alpha < e$ ist, jenachdem diese Congruenz lauter verschiedene Wurzeln hat oder auch gleiche Wurzeln zulässt. Mit $b_1, b_2, \ldots b_{q-\alpha}$ mögen die übrigen Glieder eines vollständigen Restensystems (mod. q) bezeichnet werden. Dann kann man die Congruenz (11) für jeden ganzzahligen Werth des y in dieser Weise darstellen:

$$(\eta_h - a_1)(\eta_h - a_2) \ldots (\eta_h - a_\alpha) \cdot (\eta_h - b_1)(\eta_h - b_2) \ldots (\eta_h - b_{q-\alpha}) \equiv 0 \pmod{q},$$

dafür aber einfacher auch

$$(14) \qquad (\eta_h - a_1)(\eta_h - a_2) \ldots (\eta_h - a_\alpha) \equiv 0 \pmod{q}$$

setzen, denn, da $\eta_h - x$ ein Factor von $F(x)$, also $\eta_h - b_1$, $\eta_h - b_2, \ldots \eta_h - b_{q-\alpha}$ resp. Factoren von den Functionswerthen $F(b_1), F(b_2), \ldots F(b_{q-\alpha})$ sind, so ergiebt sich aus der vorhergehenden Congruenz die folgende:

$$(\eta_h - a_1)(\eta_h - a_2) \ldots (\eta_h - a_\alpha) \cdot F(b_1) F(b_2) \ldots F(b_{q-\alpha}) \equiv 0 \pmod{q},$$

in welcher man die durch q nicht theilbaren ganzzahligen Factoren $F(b_1), F(b_2) \ldots F(b_{q-\alpha})$ unterdrücken kann.

Nachdem dies gezeigt worden, wollen wir aus der Reihe von Grössen:

$$(15) \qquad \begin{cases} \eta_0 - a_1, \; \eta_0 - a_2, \; \ldots \; \eta_0 - a_\alpha \\ \eta_1 - a_1, \; \eta_1 - a_2, \; \ldots \; \eta_1 - a_\alpha \\ \ldots \ldots \ldots \ldots \\ \eta_{e-1} - a_1, \; \eta_{e-1} - a_2, \; \ldots \; \eta_{e-1} - a_\alpha \end{cases}$$

ein Product bilden, welches die Eigenschaften hat, dass es durch q nicht theilbar ist, jeden der Factoren von der Form $\eta_h - a_i$ nur einmal enthält, und die möglichst grosse Anzahl solcher Factoren in sich vereinigt.*) Offenbar wird man ein solches Product finden, wenn man erst aus der ersten Horizontalreihe möglichst viele Factoren mit einander verbindet, deren wenigstens einer der Congruenz (14) wegen nicht mehr wird genommen werden dürfen, und sodann aus jeder der folgenden Reihen jedes Glied hinzunimmt oder verwirft, jenachdem es das schon gebildete Product durch q theilbar machen würde oder nicht.

---

*) Vgl. hierzu Kummer, über die den Gaussischen Perioden der Kreistheilung entsprechenden Congruenzwurzeln, in Cr. J. Bd. 53.

Bezeichne $\psi(\eta_0)$ ein so gebildetes Product. Dann sind die conjugirten Grössen $\psi(\eta_1), \psi(\eta_2), \ldots . \psi(\eta_{e-1})$, welche durch cyclische Vertauschung der Perioden oder, was dasselbe sagt, der Horizontalreihen (15) daraus hervorgehen, offenbar ebensolche Producte. Denn diese enthalten erstens genau soviel Factoren, wie $\psi(\eta_0)$, sind offenbar durch q nicht theilbar, wenn es $\psi(\eta_0)$ nicht ist, gestatten aber auch nicht, noch mehr der Grössen (15) hinzuzunehmen, denn, ist $\eta_{h+k} - a_i$ eine nicht in $\psi(\eta_h)$ enthaltene Grösse, welche man noch als Factor wählen kann, ohne dass $\psi(\eta_h) \,.\, (\eta_{h+k} - a_i)$ durch q theilbar würde, so wäre auch die conjugirte Grösse $\psi(\eta_0) \,.\, (\eta_k - a_i)$ nicht durch q theilbar, während $\eta_k - a_i$ ein nicht in $\psi(\eta_0)$ befindlicher Factor wäre, gegen die Bildungsweise des Products $\psi(\eta_0)$.

Die e conjugirten Functionen $\psi(\eta_0), \psi(\eta_1), \ldots . \psi(\eta_{e-1})$ sind alle von einander verschieden. Angenommen nämlich, es wäre $\psi(\eta_h) = \psi(\eta_{h+k})$ und $\eta_i - a$ ein Glied der $(i+1)^{ten}$ Horizontalreihe, welches nicht zu $\psi(\eta_h)$ gehört, wie es deren wegen der Congruenz (14) wenigstens eins geben muss, so folgte

$$\psi(\eta_h) \,.\, (\eta_i - a) \equiv 0 \pmod{q},$$

also auch die conjugirte Zahl

$$\psi(\eta_{h+k}) \,.\, (\eta_{k+i} - a) \equiv 0 \pmod{q}$$

und nach der angenommenen Gleichheit auch

$$\psi(\eta_h) \,.\, (\eta_{k+i} - a) \equiv 0 \pmod{q},$$

welche Congruenz, mit der zweitvorhergehenden verbunden, die folgende liefert, welche für jeden Werth des i besteht:

$$\psi(\eta_h) \,.\, (\eta_i - \eta_{k+i}) \equiv 0 \pmod{q}.$$

Hieraus findet man leicht eine andere, welche nicht bestehen kann, indem man mit r^{-g^i} multiplicirt und die Summe für alle Werthe des $i = 0, 1, 2, \ldots . p - 2$ bildet. Denn so ergiebt sich

$$\psi(\eta_h) \,.\, \left(\sum_{i=0}^{i=p-2} \eta_i r^{-g^i} - \sum_{i=0}^{i=p-2} \eta_{k+i}\, r^{-g^i} \right) \equiv 0 \pmod{q};$$

da nun

$$\eta_i\, r^{-g^i} = 1 + r^{g^i(g^e-1)} + r^{g^i(g^{2e}-1)} + \ldots . + r^{g^i(g^{(f-1)e}-1)}$$

und, wenn r^m nicht Eins ist, $\sum_{i=0}^{i=p-2} r^{mg^i} = -1$ ist, so findet man

$$\sum_{i=0}^{i=p-2} \eta_i\, r^{-g^i} = p-1 + \sum_{i=0}^{i=p-2} r^{(g^e-1)g^i} + \sum_{i=0}^{i=p-2} r^{(g^{2e}-1)g^i} + \dots\dots$$

$$+ \sum_{i=0}^{i=p-2} r^{(g^{(f-1)e}-1)g^i} = p-1-(f-1) = p-f,$$

ebenso, da

$$\eta_{k+i} \,.\, r_i^{-g^i} = r^{(g^k-1)g^i} + r^{(g^{e+k}-1)g^i} + \dots\dots + r^{(g^{(f-1)e+k}-1)g^i}$$

ist,

$$\sum_{i=0}^{i=p-2} \eta_{i+k} \,.\, r^{-g^i} = -f.$$

Hiernach nimmt die obige Congruenz folgende einfache Gestalt an:

$$p \,.\, \psi(\eta_h) \equiv 0 \pmod{q},$$

aus welcher die Ungereimtheit der Annahme hervorgeht. Demnach sind die e conjugirten Functionen von einander verschieden.

Endlich lässt sich zeigen, dass es ausser ihnen keine ähnlich gebildete und mit denselben Eigenschaften begabte Function mehr giebt. Denn, wäre $\varphi(\eta_0)$ eine solche, so müsste sie, da sie mit keiner der Functionen $\psi(\eta_0)$, $\psi(\eta_1) \dots\dots \psi(\eta_{e-1})$ übereinstimmt, mindestens eine der Grössen (15) zum Factor haben, welche nicht in $\psi(\eta_0)$, mindestens eine, die nicht in $\psi(\eta_1)$ enthalten ist, u. s. w., sodass für jedes h

$$\varphi(\eta_0) \,.\, \psi(\eta_h) \equiv 0 \pmod{q},$$

also auch

$$(16) \quad \varphi(\eta_0)\,(\psi(\eta_0) + \psi(\eta_1) + \dots\dots + \psi(\eta_{e-1})) \equiv 0 \pmod{q}$$

sein müsste. Die Summe innerhalb der Klammer ist als ganze und ganzzahlige symmetrische Function der Perioden einer ganzen Zahl gleich, von der leicht nachzuweisen ist, dass sie durch q nicht theilbar ist. Sonst würde nämlich auch

$$\psi(\eta_0)^{q-1}\,(\psi(\eta_0) + \psi(\eta_1) + \dots\dots + \psi(\eta_{e-1})) \equiv 0 \pmod{q}$$

sein, welche Congruenz man vermöge der Bemerkung, dass das Product zweier der e Functionen ψ, der Bedeutung derselben gemäss, jedenfalls durch q theilbar ist, auf die einfachere Gestalt:

$$(17) \quad \psi(\eta_0)^q \equiv 0 \pmod{q}$$

reduciren kann. Setzt man nun

$$\psi(\eta_0) = A_0\eta_0 + A_1\eta_1 + \ldots + A_{e-1}\eta_{e-1},$$

wo die Coëfficienten ganze Zahlen sein müssen, da $\psi(\eta_0)$ nur Factoren der Reihen (15) enthält, so ist nach dem polynomischen Satze:

$$\psi(\eta_0)^q \equiv A_0^q\eta_0^q + A_1^q\eta_1^q + \ldots + A_{e-1}^q\eta_{e-1}^q \pmod{q}$$

oder nach Fermat's Satze und da nach (6) $\eta_h^q \equiv \eta_{h+k} \equiv \eta_h$ ist, für eine zum Exponenten f gehörige Primzahl q,

$$\psi(\eta_0)^q \equiv A_0\eta_0 + A_1\eta_1 + \ldots + A_{e-1}\eta_{e-1} \equiv \psi(\eta_0).$$

Die Congruenz (17) führt demnach zu der andern: $\psi(\eta_0) \equiv 0 \pmod{q}$, welche nicht stattfindet. Da also in (16) der zweite Factor durch q nicht theilbar ist, müsste es der erste Factor sein, was der Bedeutung des Zeichens $\varphi(\eta_0)$ widerstreitet.

6. Nach diesen Vorbemerkungen ist es nunmehr möglich, zwischen den Perioden $\eta_0, \eta_1, \eta_2, \ldots \eta_{e-1}$ d. h. den Wurzeln der Gleichung $F(x) = 0$ und den Wurzeln der Congruenz $F(x) \equiv 0 \pmod{q}$ eine bestimmte Zusammengehörigkeit festzustellen. Dazu dient jede der Functionen $\psi(\eta_0), \psi(\eta_1), \ldots, \psi(\eta_{e-1})$. In der That, nehmen wir irgend eine dieser Functionen, z. B. $\psi(\eta_0)$; die Congruenz (14) hat uns gezeigt, dass sich in jeder der Horizontalreihen (15) wenigstens ein Glied befindet, welches in $\psi(\eta_0)$ nicht auftritt, es ist jedoch auch leicht zu beweisen, dass nur eins dieser Glieder in $\psi(\eta_0)$ fehlen kann. Wären nämlich die beiden Glieder $\eta_h - a$ und $\eta_h - a'$ nicht in $\psi(\eta_0)$ vorhanden, so müsste sowohl

$$\psi(\eta_0) \,.\, (\eta_h - a) \equiv 0 \text{ als auch } \psi(\eta_0) \,.\, (\eta_h - a') \equiv 0 \pmod{q}$$

sein, woraus $\psi(\eta_0) \,.\, (a - a') \equiv 0 \pmod{q}$ sich ergäbe, was nicht möglich ist, da die Werthe a, a' incongruent sind. Nennt man daher allgemein $\eta_h - u_h$ dasjenige ganz bestimmte Glied der $(h+1)^{ten}$ Horizontalreihe, welches in $\psi(\eta_0)$ sich nicht findet, so ist dasselbe durch die Congruenz

$$\psi(\eta_0) \,.\, \eta_h \equiv \psi(\eta_0) \,.\, u_h \pmod{q} \tag{18}$$

vollständig characterisirt, und so eine ganz eigenthümliche Correspondenz zwischen den Gleichungs- und Congruenzwurzeln hergestellt.

Diese Correspondenz ist freilich insofern eine nicht völlig bestimmte, als sie sich ändert mit der Function, welche wir, um

die Correspondenz herzustellen, aus der Reihe der e conjugirten Functionen auswählen. Jedoch ist einfach zu zeigen, dass, wenn bei der Zugrundelegung der Function $\psi(\eta_0)$ den Perioden

$$\eta_0, \eta_1, \eta_2 \ldots\ldots \eta_{e-1}$$

die Congruenzwurzeln

$$u_0, u_1, u_2, \ldots\ldots u_{e-1}$$

zugeordnet sind, diese Reihe nur cyclisch zu permutiren ist, sobald statt $\psi(\eta_0)$ eine der conjugirten Functionen gewählt wird. In der That, ist

$$\psi(\eta_0) \cdot \eta_h \equiv \psi(\eta_0) \cdot u_h \pmod{q},$$

so ergiebt sich durch cyclische Vertauschung der Perioden:

(19) $$\psi(\eta_k) \cdot \eta_{h+k} \equiv \psi(\eta_k) \cdot u_h \pmod{q}$$

d. h. den Perioden

$$\eta_0, \eta_1, \eta_2, \ldots\ldots \eta_{e-1}$$

sind jetzt, wenn i zur Abkürzung für $e - k$ gesetzt wird, die Congruenzwurzeln

$$u_i, u_{i+1}, u_{i+2}, \ldots\ldots u_{i-1},$$

oder umgekehrt den Congruenzwurzeln

$$u_0, u_1, u_2, \ldots\ldots u_{e-1}$$

die Perioden

$$\eta_k, \eta_{k+1}, \eta_{k+2}, \ldots\ldots \eta_{k-1}$$

zugeordnet.

Hat man eine solche Zuordnung der Congruenzwurzeln zu den Perioden hergestellt, so springen sofort sehr wichtige Analogieen zwischen Beiden hervor, welche sich in folgendem Hauptsatze aussprechen lassen: Ist $F(\eta_0, \eta_1, \ldots\ldots \eta_{e-1})$ irgend eine ganze und ganzzahlige Function der Perioden und

$$F(\eta_0, \eta_1, \ldots\ldots \eta_{e-1}) = 0,$$

so ist sofort auch

$$F(u_0, u_1, \ldots\ldots u_{e-1}) \equiv 0 \pmod{q},$$

oder: Jede ganzzahlige rationale Gleichung zwischen den Perioden geht in eine richtige Congruenz (mod. q) über, wenn statt der Perioden die zugehörigen Congruenzwurzeln gesetzt werden.

In der That, stellt man die Function der Perioden in der Normalform

$$A_0\eta_0 + A_1\eta_1 + \ldots\ldots + A_{e-1}\eta_{e-1}$$

dar, worin die Coëfficienten ganze Zahlen bedeuten, und multiplicirt mit $\psi(\eta_0)$, so folgt nach der Congruenz (18)

$$\psi(\eta_0)(A_0\eta_0 + A_1\eta_1 + \ldots + A_{e-1}\eta_{e-1}) \equiv \psi(\eta_0)(A_0 u_0 + A_1 u_1 + \ldots + A_{e-1}u_{e-1})$$

und folglich, wenn die Gleichung

$$F(\eta_0, \eta_1, \ldots \eta_{e-1}) = A_0\eta_0 + A_1\eta_1 + \ldots + A_{e-1}\eta_{e-1} = 0$$

erfüllt wird, auch die Congruenz

$$F(u_0, u_1, \ldots u_{e-1}) = A_0 u_0 + A_1 u_1 + \ldots + A_{e-1}u_{e-1} \equiv 0 \pmod{q},$$

da $\psi(\eta_0)$ nicht durch q theilbar ist, w. z. b. w.

Von den Beispielen, welche zu diesem Satze sich darbieten, begnügen wir uns, ein einziges hier anzufügen, welches im Folgenden eine wichtige Rolle spielen wird. Bezeichnen wir mit $f(\eta_0)$ irgend eine ganze und ganzzahlige Function der Perioden, sodass wir setzen können

$$f(\eta_0) = A_0\eta_0 + A_1\eta_1 \ldots + A_{e-1}\eta_{e-1},$$

während $A_0, A_1, \ldots A_{e-1}$ ganze Zahlen bedeuten, und mit $f(\eta_1), f(\eta_2) \ldots f(\eta_{e-1})$ die hierzu conjugirten, nämlich durch cyclische Vertauschung der Perioden daraus hervorgehenden Ausdrücke, so ist das Product

$$f(\eta_0) \cdot f(\eta_1) \ldots f(\eta_{e-1}),$$

welches kurz durch $Nf(\eta_0)$ bezeichnet werde, nach Nr. 6, 3) der 6. Vorlesung einer ganzen Zahl N gleich. Nach dem vorigen Satze folgt aber aus der Gleichung

$$f(\eta_0) \cdot f(\eta_1) \ldots f(\eta_{e-1}) = N$$

sofort die Congruenz

$$f(u_0) \cdot f(u_1) \ldots f(u_{e-1}) \equiv N \pmod{q},$$

worin die Factoren der linken Seite ganze reelle Zahlen sind. Hieraus erhellt der Satz:

Die durch das Product

$$Nf(\eta_0) = f(\eta_0) \cdot f(\eta_1) \ldots f(\eta_{e-1})$$

dargestellte ganze Zahl N ist durch q theilbar oder nicht theilbar, jenachdem es eine der Zahlen

$$f(u_0), f(u_1), \ldots f(u_{e-1})$$

ist oder nicht ist.

Noch sei zum Schlusse bemerkt, dass nach dem vorletzten Satze die Gleichungen in Nr. 7 der 6. Vorlesung sowie die Kummer'schen Relationen in der 15. Vorlesung, welche zwischen

den Perioden bestehen und dazu dienten, jede derselben als rationale Function einer beliebigen unter ihnen zu bestimmen, in richtige Congruenzen (mod. q) übergehen, wenn statt der Perioden die zugehörigen Congruenzwurzeln gesetzt werden. Diese Congruenzen gestatten also, wenn diejenige Congruenzwurzel bestimmt ist, welche einer gegebenen Periode zugehört, die Zusammengehörigkeit zwischen den übrigen Congruenzwurzeln und Perioden ohne Weiteres zu finden. —

Achtzehnte Vorlesung.

Die Theorie der aus Einheitswurzeln gebildeten complexen ganzen Zahlen.

1. Wir wenden uns nun zu den, aus den Wurzeln der Gleichung $x^p = 1$ gebildeten complexen ganzen Zahlen. Nach der 6. Vorlesung Nr. 3 kann jede ganze Function von den Wurzeln dieser Gleichung auf die ganz bestimmte Form

$$A_1 r + A_2 r^2 + \dots + A_{p-1} r^{p-1}$$

gebracht werden. Jeder Ausdruck dieser Art, in welchem die Coëfficienten ganze Zahlen sind, soll eine, aus den p^{ten} Einheitswurzeln gebildete complexe ganze Zahl oder im Folgenden kurz eine complexe Zahl genannt werden. Wir setzen:

$$f(r) = A_1 r + A_2 r^2 + \dots + A_{p-1} r^{p-1}. \tag{1}$$

Ersetzt man r durch die sämmtlichen primitiven Wurzeln der Gleichung $x^p = 1$, so erhält man die $p-1$ conjugirten complexen Zahlen

$$f(r),\ f(r^2),\ f(r^3),\ \dots\ f(r^{p-1}),$$

deren Product ihre gemeinschaftliche Norm heissen und durch $\mathrm{N}f(r)$ bezeichnet werden soll. Es ist also

$$\mathrm{N}f(r) = f(r)\,.\,f(r^2)\,\dots\,f(r^{p-1}) \tag{2}$$

oder auch, wenn g eine primitive Wurzel (mod. p) ist,

$$\mathrm{N}f(r) = f(r)\,.\,f(r^g)\,.\,f(r^{g^2})\,\dots\,f(r^{g^{p-2}})\,. \tag{3}$$

Die Coëfficienten A_i in $f(r)$ können so beschaffen sein, dass darin die Wurzeln $r, r^2, r^3, \dots r^{p-1}$ sich zu e Perioden von f Gliedern gruppiren, die complexe Zahl also die Gestalt

(4) $$f(r) = m_0\eta_0 + m_1\eta_1 + \ldots + m_{e-1}\eta_{e-1}$$

annimmt; in diesem Falle soll sie durch $f(\eta_0)$ bezeichnet, und als ihre conjugirten Zahlen diejenigen $e - 1$ Zahlen $f(\eta_1)$, $f(\eta_2), \ldots f(\eta_{e-1})$ betrachtet werden, welche durch cyclische Vertauschung der Perioden daraus hervorgehen, als ihre Norm aber, wie am Ende der vorigen Vorlesung, das Product

(5) $$Nf(\eta_0) = f(\eta_0) \cdot f(\eta_1) \ldots f(\eta_{e-1}) \,.$$

Zum Unterschiede wird das, aus $f(\eta_0)$ nach der Formel (2) gebildete Product dann die vollständige Norm der complexen Zahl $f(\eta_0)$ genannt werden; da in diesem Falle

$$f(r) = f(\eta_0),\ f(r^g) = f(\eta_1),\ f(r^{g^2}) = f(\eta_2), \ldots f(r^{g^{e-1}}) = f(\eta_{e-1})$$

und allgemein

$$f(r^{g^{ke+h}}) = f(r^{g^h}) = f(\eta_h)$$

ist, schliesst man offenbar die Gleichung

(6) $$\mathrm{N}f(\eta_0) = [Nf(\eta_0)]^f,$$

in Worten: die vollständige Norm einer complexen Zahl, welche aus den e Perioden von f Gliedern zusammengesetzt ist, ist gleich der f^{ten} Potenz ihrer auf die Perioden bezüglichen Norm.

Sowohl $\mathrm{N}f(r)$ als $Nf(\eta_0)$. sind übrigens als symmetrische Functionen der Wurzeln der Kreistheilungsgleichung offenbar ganze reelle Zahlen.

Jede ganze complexe Zahl $f(r)$, deren Norm der Einheit gleich ist, für welche also die Gleichung

(7) $$\mathrm{N}f(r) = 1$$

besteht, soll eine complexe Einheit genannt und mit $E(r)$ bezeichnet werden.

Zwischen den Zahlen von den beiden Formen $f(r)$, $f(\eta_0)$ findet das beachtenswerthe Verhältniss statt, dass die letztern zwar als specielle Gattung in der erstern enthalten sind, dass aber, unter einem andern Gesichtspunkt, auch die erstern als eine besondere, in den zweiten enthaltene, Gattung angesehen werden können, welche daraus hervorgeht, wenn $e = p - 1$, $f = 1$ gesetzt, nämlich die η als eingliedrige Perioden vorausgesetzt werden. Die Theorie der letztern Zahlen involvirt daher die von jenen als besonderen Fall.

Endlich muss hier noch bemerkt werden, in welcher Weise

Congruenzen verstanden werden sollen, welche zwischen complexen Zahlen stattfinden; es soll aber, ähnlich wie in Nr. 1 der vorigen Vorlesung, festgesetzt werden, dass zwei complexe Zahlen $f(r)$, $f'(r)$ (mod. q) congruent heissen sollen, wenn in den auf die Normalform gebrachten Ausdrücken $f(r)$, $f'(r)$ die Coëfficienten gleicher Potenzen von r einander (mod. q) congruent sind.

2. Nehmen wir q als eine von p verschiedene Primzahl an, so dürfen wir voraussetzen, q gehöre (mod. p) zum Exponenten f, da man nur nöthig hat, f alle Divisoren von $p-1$ durchlaufen zu lassen, um allen Primzahlen q gerecht zu werden. Ist nun

$$f(r) = A_1 r + A_2 r^2 + \ldots . + A_{p-1} \,.\, r^{p-1}$$

irgend eine aus p^{ten} Einheitswurzeln gebildete, complexe Zahl, so erhält man durch Erhebung zur q^{ten} Potenz die Congruenz

$$f(r)^q \equiv A_1{}^q r^q + A_2{}^q r^{2q} + \ldots . + A_{p-1}{}^q \,.\, r^{(p-1)q} \equiv A_1 r^q + A_2 r^{2q} + \ldots . + A_{p-1} r^{(p-1)q}$$

oder einfacher

$$(8) \qquad f(r)^q \equiv f(r^q) \text{ (mod. } q),$$

folglich durch wiederholte Erhebung in die q^{te} Potenz nachstehende Reihe von Congruenzen:

$$(9) \quad f(r) \equiv f(r), f(r)^q \equiv f(r^q), f(r)^{q^2} \equiv f(r^{q^2}), \ldots . f(r)^{q^{f-1}} \equiv f(r^{q^{f-1}}),$$

und durch nochmalige Erhebung in die q^{te} Potenz und Beachtung der Relationen $q^f \equiv 1$ (mod. p) und $r^p = 1$,

$$(10) \qquad f(r)^{q^f} \equiv f(r) \text{ (mod. } q).$$

Enthält die ganze complexe Zahl $f(r)$ nur die e f-gliedrigen Perioden $\eta_0, \eta_1, \ldots . \eta_{e-1}$, so wird schon die q^{te} Potenz derselben der Zahl $f(r)$ selbst (mod. q) congruent. In der That, setzt man

$$f(r) = m_0 \eta_0 + m_1 \eta_1 + \ldots . + m_{e-1} \,.\, \eta_{e-1},$$

so ergiebt sich

$$\left.\begin{aligned} f(r)^q &\equiv m_0{}^q \eta_0{}^q + m_1{}^q \eta_1{}^q + \ldots . + m_{e-1}{}^q \,.\, \eta_{e-1}{}^q \\ &\equiv m_0\, \eta_0{}^q + m_1\, \eta_1{}^q + \ldots . + m_{e-1} \,.\, \eta_{e-1}{}^q \end{aligned}\right\} \text{(mod. } q)$$

oder, da k für die hier betrachteten Primzahlen q durch e theilbar, also nach (6) der vorigen Vorlesung $\eta_h{}^q \equiv \eta_h$ (mod. q) ist, folgende Congruenz

$$(11) \qquad f(\eta_0)^q \equiv f(\eta_0) \text{ (mod. } q),$$

in der man $f(r)$, um seine Zusammensetzung auszudrücken, wieder durch $f(\eta_0)$ bezeichnet hat; allgemeiner für jeden Werth des Index h

$$(11a) \qquad f(\eta_h)^q \equiv f(\eta_h) \text{ (mod. } q).$$

Für jede Primzahl q der betrachteten Art besteht ferner der letzte Satz der vorigen Vorlesung, den wir hier folgendermassen aussprechen können:

Sind $u_0, u_1, \ldots u_{e-1}$ die den Perioden $\eta_0, \eta_1, \ldots \eta_{e-1}$ (mod. q) zugeordneten Congruenzwurzeln, so ist die Norm einer complexen Zahl $f(\eta_0)$ theilbar oder nicht theilbar durch q, jenachdem eine der Zahlen $f(u_0)$, $f(u_1), \ldots f(u_{e-1})$ es ist oder nicht.

Es giebt hiernach unendlich viel Zahlen $f(\eta_0)$, deren Normen durch eine gegebene Primzahl dieser Art theilbar sind. Denn, setzt man

$$f(\eta_0) = x_0\eta_0 + x_1\eta_1 + \ldots + x_{e-1}\eta_{e-1},$$

und bestimmt, was auf unendlich viel verschiedene Arten möglich ist, die unbestimmten ganzen Zahlen $x_0, x_1, \ldots x_{e-1}$ so, dass

$$(12) \quad f(u_0) \equiv x_0 u_0 + x_1 u_1 + \ldots + x_{e-1}u_{e-1} \equiv 0 \pmod{q}$$

wird, so ist nach dem eben ausgesprochenen Satze $Nf(\eta_0)$ durch q theilbar, etwa, wenn M eine ganze reelle Zahl bezeichnet,

$$Nf(\eta_0) = q \,.\, M.$$

Gelingt es, die ganzen Zahlen $x_0, x_1, \ldots x_{e-1}$ so zu wählen, dass in dieser Gleichung $M = 1$ wird, so ergiebt sich auf diesem Wege eine Zerlegung der reellen Primzahl q in e complexe Factoren:

$$f(\eta_0), f(\eta_1), \ldots f(\eta_{e-1}).$$

Von diesen ist leicht nachzuweisen, dass sie die Rolle von complexen Primfactoren spielen, nämlich nicht weiter in Factoren zerlegbar sind, welche von complexen Einheiten verschieden sind. In der That, wäre etwa

$$f(\eta_0) = \varphi(r) \,.\, \psi(r),$$

so ergäbe sich, wenn die vollständige Norm der Zahl $f(\eta_0)$ gebildet wird, wegen der Gleichung (6) und, weil $Nf(\eta_0) = q$ vorausgesetzt ist, folgende Gleichung:

$$q^f = \mathrm{N}\varphi(r) \,.\, \mathrm{N}\psi(r),$$

in welcher zur Rechten das Product zweier ganzer Zahlen befindlich ist. Wir werden aber sogleich nachweisen, dass die vollständige Norm einer complexen Zahl, welche durch q theilbar ist, stets durch q^f theilbar sein muss; daher kann die vorige Gleichung nur bestehen, indem man etwa annimmt

$$\mathrm{N}\varphi(r) = q^f, \; \mathrm{N}\psi(r) = 1,$$

d. h. einer der Factoren $\varphi(r)$, $\psi(r)$ ist nothwendigerweise eine complexe Einheit.

3. **Gelingt es aber nicht, die Zahlen $x_0, x_1, \ldots . x_{e-1}$ der Congruenz (12) gemäss so zu wählen, dass $M = 1$ wird, giebt es also keine Zerlegung der Primzahl q in e complexe Factoren, welche aus den Perioden $\eta_0, \eta_1, \ldots . \eta_{e-1}$ gebildet sind, so giebt es überhaupt keine Zerlegung derselben in complexe, aus p^{ten} Einheitswurzeln gebildete Factoren.** Ist nämlich

$$f(r) = A_1 r + A_2 r^2 + \ldots . + A_{p-1} r^{p-1}$$

irgend eine solche Zahl, so bestehen die Congruenzen (9), aus deren Multiplication sich

$$f(r)^{1+q+q^2+\ldots+q^{f-1}} \equiv f(r) \,.\, f(r^q) \,.\, f(r^{q^2}) \ldots . f(r^{q^{f-1}}) \pmod{q}$$

ergiebt, was sich auch, wenn $q \equiv g^{me} \pmod{p}$ gesetzt wird, so schreiben lässt:

$$f(r)^{1+q+q^2+\ldots+q^{f-1}} \equiv f(r)\, f(r^{g^{me}})\, f(r^{g^{2me}}) \ldots . f(r^{g^{(f-1)me}})$$

oder auch, da q zum Exponenten f gehört, also m nach Vorlesung 4 Nr. 10, 3) relative Primzahl zu f ist, und deshalb die Zahlen $m, 2m, \ldots . (f-1)m \pmod{f}$ den Zahlen $1, 2, 3, \ldots . f-1$ von der Reihenfolge abgesehen congruent sind,

$$f(r)^{1+q+q^2+\ldots+q^{f-1}} \equiv f(r)\, f(r^{g^e})\, f(r^{g^{2e}}) \ldots . f(r^{g^{(f-1)e}}) \pmod{q}.$$

Setzt man in dieser Congruenz für r successive r^g, $r^{g^2}, \ldots . r^{g^{e-1}}$ und multiplicirt die so entstehenden in einander, so bildet man auf der rechten Seite offenbar die vollständige Norm der complexen Zahl $f(r)$, und es geht

$$[f(r) \,.\, f(r^g) \,.\, f(r^{g^2}) \ldots . f(r^{g^{e-1}})]^{1+q+q^2+\ldots+q^{f-1}} = \mathrm{N} f(r) \pmod{q}$$

hervor. Bei der Annahme, dass $f(r)$ eine Zahl sei, deren Norm durch q theilbar ist, geht diese Congruenz in die specielle über:

$$[f(r) \,.\, f(r^g) \,.\, f(r^{g^2}) \ldots . f(r^{g^{e-1}})]^{1+q+q^2+\ldots+q^{f-1}} \equiv 0 \pmod{q}.$$

Wenn man aber diese letzte zur $(q-1)^{ten}$ Potenz erhebt, wodurch der Exponent auf der linken Seite in $q^f - 1$ übergeht, und noch einmal mit dem Ausdrucke in der Klammer multiplicirt, so gelangt man nach (10) zu dem Resultate

$$f(r)\, f(r^g) \ldots . f(r^{g^{e-1}}) \equiv 0 \pmod{q}$$

oder zu dem Satze: **Wenn die vollständige Norm der**

complexen Zahl $f(r)$ durch eine zum Exponenten f gehörige Primzahl q theilbar ist, so ist es sogar schon das Product ihrer ersten e Factoren.

Angenommen nun, dies Product sei durch q^n theilbar, so besteht die vorige Congruenz auch mod. q^n. Da man aber in derselben r durch r^{g^e}, $r^{g^{2e}}$ .... $r^{g^{(f-1)e}}$ ersetzen darf, so folgt weiter, dass je e successive Factoren der Norm durch q^n theilbar sind, also die vollständige Norm selbst durch q^{nf}.

Man findet so den Satz: Ist q eine zum Exponenten f gehörige Primzahl, so enthält die vollständige Norm einer complexen Zahl stets eine ganze Potenz von q^f als Factor, sobald sie überhaupt durch q theilbar ist.

Wäre nun q in e' conjugirt-complexe Factoren von der Form

$$f(\eta_0') = m_0\eta_0' + m_1\eta_1' \dots + m_{e'-1} \cdot \eta'_{e'-1},$$

welche aus den e' Perioden von f' Gliedern gebildet sind, zerlegbar, so ergäbe sich die vollständige Norm dieser Zahl nach (6) gleich $Nf(\eta_0')^{f'} = q^{f'}$, es müsste daher f' ein Vielfaches von f, jede der f'-gliedrigen Perioden also aus einer Anzahl der f-gliedrigen zusammengesetzt, und $f(\eta_0')$ einer complexen, aus den Perioden $\eta_0, \eta_1, \dots \eta_{e-1}$ zusammengesetzten Zahl gleich sein. Wenn demnach q nicht als Norm einer solchen dargestellt werden kann, so ist in der That ihre Zerlegung in complexe aus p^{ten} Einheitswurzeln gebildete Factoren überhaupt nicht möglich.

4. Es lässt sich nun aber auch leicht zeigen, dass eine reelle Primzahl q nicht immer in complexe Factoren zerlegbar ist. Nehmen wir z. B. eine Primzahl q von der Form $2mp + 1$, für welche $f = 1$, $e = p - 1$ ist, so muss eine solche, wenn sie überhaupt zerlegbar ist, nach dem eben Bewiesenen in $p - 1$ conjugirte Factoren zerlegbar sein, welche nur die Einheitswurzeln für sich, nicht aber zu Perioden verbunden, enthalten. Sei $f(r)$ eine solche, so müsste

$$q = f(r) \cdot f(r^g) \cdot f(r^{g^2}) \dots f(r^{g^{p-2}})$$

sein, wo man auch die $p - 1$ Factoren in zwei Gruppen von $\frac{p-1}{2}$ Factoren vertheilen und schreiben kann:

$$q = f(r)\, f(r^{g^2}) \dots f(r^{g^{p-3}}) \cdot f(r^g)\, f(r^{g^3}) \dots f(r^{g^{p-2}}).$$

Die hierin enthaltenen beiden Producte sind ganze und ganzzahlige symmetrische Functionen der, in je einer der beiden

$\frac{p-1}{2}$ gliedrigen Perioden, welche η_0, η_1 heissen mögen, enthaltenen Wurzeln, also kann nach Nr. 5 der 6. Vorlesung

$$f(r) \cdot f(r^{g^2}) \ldots . f(r^{g^{p-3}}) = A_0 \eta_0 + A_1 \eta_1$$
$$f(r^g) \cdot f(r^{g^3}) \ldots . f(r^{g^{p-2}}) = A_0 \eta_1 + A_1 \eta_0$$

gesetzt werden. Hierin haben aber die Perioden η_0, η_1 nach Nr. 2 der 15. Vorlesung die Werthe

$$\eta_0 = \frac{-1 + \sqrt{(-1)^{\frac{p-1}{2}} \cdot p}}{2}, \quad \eta_1 = \frac{-1 - \sqrt{(-1)^{\frac{p-1}{2}} \cdot p}}{2},$$

folglich findet man durch Substitution in die vorigen Gleichungen und durch deren Multiplication

$$q = \left[-\frac{A_0 + A_1}{2} + \frac{A_0 - A_1}{2} \cdot \sqrt{(-1)^{\frac{p-1}{2}} \cdot p} \right]$$
$$\left[-\frac{A_0 + A_1}{2} - \frac{A_0 - A_1}{2} \cdot \sqrt{(-1)^{\frac{p-1}{2}} \cdot p} \right]$$

oder

$$4q = (A_0 + A_1)^2 - (-1)^{\frac{p-1}{2}} p \cdot (A_0 - A_1)^2 .$$

Soll also q zerlegbar sein, so muss $4q$ durch die quadratische Form

$$x^2 - (-1)^{\frac{p-1}{2}} p \cdot y^2$$

darstellbar sein, was nach der Theorie der quadratischen Formen keineswegs immer der Fall ist.

5. Soweit verhält sich in der Theorie der hier betrachteten complexen Zahlen Alles ganz analog, wie bei den complexen Zahlen von einer der beiden Formen $a + bi$ und $a + b\varrho$, welche wir früher untersucht haben: Alle reellen Primzahlen zerfallen in zwei Klassen, von diesen enthält die eine diejenigen, welche nicht weiter zerlegbar sind, die andere diejenigen, welche in complexe Factoren zerfallen, die sodann die Rolle wirklicher Primfactoren in der complexen Zahlentheorie vertreten. Nunmehr aber muss auf einen capitalen Unterschied dieser Theorie von jenen früheren aufmerksam gemacht werden: jene erstern, nicht weiter in complexe Factoren zerlegbaren Primzahlen dürfen hier nicht, wie dort, als

Primfactoren angesehen werden. Dies zeigt sich unmittelbar in dem Umstande, dass der Hauptsatz, nach welchem jede complexe Zahl nur auf eine Weise als Product der Primfactoren darstellbar ist, seine Geltung für die eben genannten Primzahlen verliert. Um davon eine einfache Probe zu liefern, sei q eine Primzahl von der Form $2mp + 1$, welche nicht in complexe Factoren zerlegbar ist. Da nach dem ersten Satze in Nr. 4 der vorigen Vorlesung die Congruenz

$$x^{p-1} + x^{p-2} + \ldots . + x + 1 \equiv 0 \pmod{q}$$

$p - 1$ reelle Wurzeln hat, so sei $x \equiv u$ eine derselben. Betrachten wir sodann die complexe ganze Zahl $f(r) = u - r$, so findet man

$$\mathrm{N}f(r) = (u-r)(u-r^2)(u-r^3) \ldots (u-r^{p-1}) = u^{p-1} + u^{p-2} + \ldots + 1$$

d. h. gleich einer durch q theilbaren ganzen Zahl $q . M$, also die Gleichung

$$(u - r)(u - r^2) \ldots . (u - r^{p-1}) = q . M.$$

Wäre nun q ein wahrer Primfactor, so müsste er in einem der complexen Factoren als Divisor aufgehen, was doch offenbar nicht sein kann.

6. Dieser Umstand, durch welchen die ganze Theorie der hier betrachteten complexen Zahlen sehr schwierig und unvollkommen wird, könnte es zweifelhaft machen, ob sie überhaupt ein ähnliches Interesse beanspruchen können, als die früher betrachteten einfacheren Gattungen complexer Zahlen.

Indessen ist es Kummer gelungen, durch Einführung sogenannter idealer complexer Primfactoren die Analogie mit den reellen und jenen einfacheren complexen Zahlen vollständig wiederherzustellen und so eigentlich erst die innere Natur der, aus Einheitswurzeln höheren Grades gebildeten complexen Zahlen aufzuschliessen. Durch solche Einführung idealer Factoren wird offenbar ein ganz ähnliches Bedürfniss der mathematischen Speculation befriedigt, wie durch Einführung der imaginären Wurzeln, welche den Fundamentalsätzen der Algebra, namentlich dem Satze, dass jede Gleichung ebensoviel Wurzeln zulasse, als ihr Grad beträgt, unbedingte Allgemeinheit verschaffen, oder wie durch die Zulassung der complexen Zahlen $a + bi$ bei den biquadratischen, der Zahlen $a + b\varrho$ bei den cubischen Resten, ja der Zahlen von der Form $f(r)$ selber in der Theorie der

höheren Potenzreste, welche in allen diesen Fällen resp. erst die eigentlichen Elemente der Untersuchung bilden.

Um die wahre Bedeutung solcher Erweiterung eines mathematischen Begriffes in das richtige Licht zu setzen, bedient sich Kummer eines Beispiels, welches dazu sehr geeignet ist. Zwei Kreise, welche sich schneiden, haben bekanntlich zwei Punkte gemeinschaftlich, durch welche eine Gerade, die sogenannte gemeinschaftliche Sehne bestimmt wird. Wenn die beiden Kreise aufhören, sich wirklich zu schneiden, kann von einer reellen gemeinschaftlichen Sehne natürlich nicht mehr die Rede sein. Dennoch giebt es eine gewisse reelle Gerade, welche auch in diesem Falle zu den Kreisen dasselbe Verhältniss beibehält, das in dem Falle des Durchschneidens derselben die gemeinschaftliche Sehne besitzt, wenn man nicht ihre Eigenschaft, durch die Durchschnittspunkte zu gehen, sondern jene andere, ihr zukommende Eigenschaft, dass die, von ihren Punkten an beide Kreise gelegten Tangenten gleiche Länge haben, als die wesentliche, characteristische Eigenschaft betrachtet. Legt man diese bleibende Eigenschaft zu Grunde, so hat die gemeinschaftliche Sehne eine reale Existenz, gleichviel, ob die Kreise die zufällige Eigenschaft haben, sich zu schneiden, oder nicht, obwohl sie eine ideale Sehne genannt werden muss, wenn die Kreise dieser zufälligen Eigenschaft ermangeln.

Gelingt es uns hiernach, die bisherige Definition der complexen Primzahlen als einfachste Factoren, in welche die reellen Primzahlen zerlegbar sind, durch eine andere zu ersetzen, welche ihre Geltung beibehält, gleichviel, ob die reellen Primzahlen q in wirkliche complexe Factoren zerlegt werden können oder nicht, so wird der so definirte Begriff in beiden Fällen eine reale Existenz haben. Will man aber für denselben den Namen „Primfactor" beibehalten, auch wenn der zufällige Umstand der Zerlegbarkeit von q nicht stattfindet, so wird dieser Primfactor eben als ein idealer bezeichnet werden müssen. Im Grunde ist hier also nirgends etwas Imaginäres, als in der Bezeichnung.

7. Nach den vorher gefundenen Resultaten ist es nun leicht, eine umfassendere Definition der bezeichneten Art für die idealen Primfactoren zu finden. Nehmen wir an, q sei eine zum Exponenten f (mod. p) gehörige Primzahl, welche in e conjugirte complexe Factoren $f(\eta_0), f(\eta_1), \ldots . f(\eta_{e-1})$ zerlegbar ist, und

$F(r)$ eine complexe, durch einen dieser Factoren theilbare Zahl, und sehen zu, wie sich dieser Umstand durch Congruenzbedingungen ausdrücken lässt, wenn man die Zusammengehörigkeit der Perioden und Congruenzwurzeln benutzt. Dazu erinnere man sich zuerst, dass die f Wurzeln, welche die Periode η_0 zusammensetzen, nach Nr. 8 der 6. Vorlesung einer irreductibeln Gleichung Genüge leisten, deren Coëfficienten ganze und ganzzahlige Functionen von den Perioden sind; sie werde durch

$$z^f + M_1 z^{f-1} + \ldots . + M_f = 0 \tag{13}$$

bezeichnet, sodass identisch

$$r^f + M_1 r^{f-1} + \ldots . M_f = 0$$

ist. Mit Hilfe dieser Gleichheit können leicht aus der complexen Zahl $F(r)$ alle höheren Potenzen von r als die $(f-1)^{te}$ entfernt, also $F(r)$ auf folgende Form:

$$F(r) = C_0 + C_1 r + C_2 r^2 + \ldots . + C_{f-1} \,.\, r^{f-1} \tag{14}$$

gebracht werden, in welcher die Coëfficienten $C_0, C_1, \ldots . C_{f-1}$ ganze und ganzzahlige Functionen der Perioden sind, und deshalb durch

$$C_0 = \varphi(\eta_0),\ C_1 = \varphi_1(\eta_0), \ldots . C_{f-1} = \varphi_{f-1}(\eta_0) \tag{15}$$

bezeichnet werden mögen. Soll nun, wie vorausgesetzt wurde, $F(r)$ etwa den Factor $f(\eta_h)$ von q enthalten, so kann dies wegen der Irreductibilität der Gleichung (13) nicht anders geschehen, als wenn alle Coëfficienten in dem Ausdrucke (14) diesen Factor enthalten. Man darf dann setzen:

$$\varphi(\eta_0) = f(\eta_h) \,.\, \varphi'(\eta_0),\ \varphi_1(\eta_0) = f(\eta_h) \,.\, \varphi_1'(\eta_0), \ldots . \varphi_{f-1}(\eta_0) = f(\eta_h) \,.\, \varphi'_{f-1}(\eta_0). \tag{16}$$

Andererseits bemerke man, dass nach der Annahme

$$f(\eta_0)\, f(\eta_1) \ldots . f(\eta_{e-1}) = q$$

ist, folglich nach dem ersten Satze in Nr. 2 eine der Zahlen $f(u_0), f(u_1), \ldots . f(u_{e-1})$, etwa $f(u_{h+i})$ durch q theilbar sein muss. Denkt man sich nun, indem $k = e - i$ gesetzt wird, die Congruenzwurzeln in der bestimmten Weise den Perioden zugeordnet, wie es in Nr. 6 der vorigen Vorlesung der Congruenz (19):

$$\psi(\eta_k) \,.\, (\eta_{h+k} - u_h) \equiv 0 \pmod{q}$$

gemäss geschehen ist, so werden die Gleichungen (16) folgende f Congruenzen:

(17) $\varphi(u_i) \equiv f(u_{h+i}) . \varphi'(u_i) \equiv 0, \dots \varphi_{f-1}(u_i) \equiv f(u_{h+i}) . \varphi'_{f-1}(u_i) \equiv 0$
nach sich ziehen, welche demnach die Bedingung ausdrücken, dass $F(r)$ den Factor $f(\eta_h)$ von q enthalte, welchen wir den zur Substitution $\begin{pmatrix}\eta_h \\ u_{h+i}\end{pmatrix}$ oder $\begin{pmatrix}\eta_{h+k} \\ u_h\end{pmatrix}$ gehörigen nennen wollen.

Man kann dieselben einfacher in eine einzige Congruenz zusammenfassen. In der That, ihnen zufolge ist

$$\varphi(u_i) + \varphi_1(u_i) . r + \varphi_2(u_i) . r^2 + \dots + \varphi_{f-1}(u_i) . r^{f-1}$$

ein Ausdruck mit lauter durch q theilbaren Coëfficienten, dasselbe gilt also auch, wenn wir ihn mit $\psi(\eta_k)$ multipliciren, wodurch hervorgeht:

$$\varphi(u_i) . \psi(\eta_k) + \varphi_1(u_i) . \psi(\eta_k) . r + \dots + \varphi_{f-1}(u_i) . \psi(\eta_k) . r^{f-1} \equiv 0 \pmod{q}.$$

Da aber wegen (19) der vorigen Vorlesung sich

$$\varphi(u_i) . \psi(\eta_k) \equiv \varphi(\eta_0) . \psi(\eta_k), \dots \varphi_{f-1}(u_i) . \psi(\eta_k) \equiv \varphi_{f-1}(\eta_0) . \psi(\eta_k) \pmod{q}$$

ergiebt, so können die f Congruenzen (17) in die nachstehende einzige zusammengezogen werden:

$$F(r) . \psi(\eta_k) \equiv 0 \pmod{q}. \tag{18}$$

Diese drückt daher die Bedingung aus, unter welcher $F(r)$ den zur Substitution $\begin{pmatrix}\eta_{h+k} \\ u_h\end{pmatrix}$ gehörigen complexen Factor von q als Factor enthalten kann.

Die soeben als nothwendig erkannte Congruenzbedingung ist auch hinreichend, um die Theilbarkeit von $F(r)$ durch einen Primfactor von q zu sichern. Denn sie ergiebt, wenn sie stattfindet, die Gleichung

$$F(r) . \psi(\eta_k) = q . \Psi(r)$$

oder

$$F(r) . \psi(\eta_k) = f(\eta_0) . f(\eta_1) \dots f(\eta_{e-1}) . \Psi(r),$$

in welcher man auch die Function $\Psi(r)$ vermittelst der Gleichung (13) unter den Grad f erniedrigt und so auf die Form

$$k_0 + k_1 r + \dots + k_{f-1} . r^{f-1}$$

gebracht annehmen darf, sodass dann die Coëfficienten gleicher Potenzen von r auf beiden Seiten einzeln gleichzusetzen sind. So findet man

$$\varphi(\eta_0)\psi(\eta_k) = f(\eta_0) \dots f(\eta_{e-1}) . k_0, \dots \varphi_{f-1}(\eta_0)\psi(\eta_k) = f(\eta_0) \dots f(\eta_{e-1}) . k_{f-1}.$$

Da nun $\psi(\eta_k)$ nicht durch q theilbar ist, muss mindestens einer der Primfactoren von q, etwa $f(\eta_h)$, in allen Functionen

$\varphi(\eta_0)$, $\varphi_1(\eta_0)$, ... $\varphi_{f-1}(\eta_0)$, d. h. in $F(r)$ als Factor enthalten sein, w. z. b. w.

Nun enthält aber die Congruenz (18) keine Spur mehr von der Annahme, dass q wirklich in complexe Factoren zerlegbar sei, drückt also eine Eigenschaft aus, welche ebensowohl auch den nicht zerlegbaren Primzahlen zukommen kann, und kann daher zur Definition der idealen Primfactoren gewählt werden. Diese stellen wir nunmehr folgendermassen auf:

Definition. Ist für eine complexe Zahl $F(r)$ die Congruenz

(18) $$\psi(\eta_k) \,.\, F(r) \equiv 0 \pmod{q}$$

erfüllt, so soll gesagt werden, sie enthalte den zur Substitution $\binom{\eta_{h+k}}{u_h}$ gehörigen idealen Primfactor des q. Besteht aber die Congruenz

(19) $$\psi(\eta_k)^m \,.\, F(r) \equiv 0 \pmod{q^m},$$

jedoch nicht mehr die folgende:

$$\psi(\eta_k)^{m+1} \,.\, F(r) \equiv 0 \pmod{q^{m+1}},$$

so werden wir sagen, die complexe Zahl enthalte jenen Primfactor genau m Mal.

8. Von den, so als Congruenzbedingungen definirten, idealen Primfactoren lässt sich nun leicht nachweisen, dass sie alle wesentlichen Eigenschaften gewöhnlicher Primzahlen besitzen. Vor Allem gilt folgender Fundamentalsatz:

1) Sind $f(r)$, $\varphi(r)$ zwei complexe Zahlen, welche den zur Substitution $\binom{\eta_{h+k}}{u_h}$ gehörigen idealen Primfactor der reellen Primzahl q nicht enthalten, so enthält auch ihr entwickeltes Product diesen Factor nicht.

Nach der Voraussetzung sind die beiden Ausdrücke

$$\psi(\eta_k) \,.\, f(r) \text{ und } \psi(\eta_k) \,.\, \varphi(r)$$

nicht durch q theilbar. Nun bestehen aber, wenn $q \equiv g^{me} \pmod{p}$ gesetzt wird, nach (8) und (11a) folgende Congruenzen:

$$\left.\begin{array}{l} \psi(\eta_k) \,.\, f(r) \equiv \psi(\eta_k) \,.\, f(r) \\ \psi(\eta_k)^q \,.\, f(r)^q \equiv \psi(\eta_k) \,.\, f(r^{g^{me}}) \\ \psi(\eta_k)^{q^2} \,.\, f(r)^{q^2} \equiv \psi(\eta_k) \,.\, f(r^{g^{2me}}) \\ \cdots\cdots\cdots\cdots \\ \psi(\eta_k)^{q^{f-1}} . f(r)^{q^{f-1}} \equiv \psi(\eta_k) . f(r^{g^{(f-1)me}}) \end{array}\right\} \pmod{q},$$

deren Multiplication zu der nachstehenden:

$$[\psi(\eta_k) \,.\, f(r)]^{1+q+q^2+\cdots+q^{f-1}} \equiv \psi(\eta_k)^f \,.\, F(\eta_0) \pmod{q}$$

hinführt, wenn für das Product

$$f(r) \,.\, f(r^{g^{me}}) \,\ldots\, . \, f(r^{g^{(f-1)me}}),$$

welches offenbar nur von den e f-gliedrigen Perioden abhangt, das Zeichen $F(\eta_0)$ gesetzt wird. Diese Congruenz lehrt aber, dass $\psi(\eta_k) \,.\, F(\eta_0)$ nicht durch q theilbar sein kann, weil sonst auch

$$[\psi(\eta_k) \,.\, f(r)]^{1+q+q^2+\cdots+q^{f-1}} \equiv 0 \pmod{q},$$

folglich auch

$$\psi(\eta_k) \,.\, f(r) \equiv 0 \pmod{q}$$

sein müsste, wie man findet, wenn man zur $(q-1)^{ten}$ Potenz erhebt, sodann noch einmal mit $\psi(\eta_k) \,.\, f(r)$ multiplicirt und die Congruenz

$$[\psi(\eta_k) \,.\, f(r)]^{q^f} \equiv \psi(\eta_k) \,.\, f(r) \pmod{q}$$

beachtet.

Ganz ähnlich findet man, wenn

$$\varphi(r) \,.\, \varphi(r^{g^{me}}) \,\ldots\, . \,\varphi(r^{g^{(f-1)me}}) = \Phi(\eta_0)$$

gesetzt wird, dass auch $\psi(\eta_k) \,.\, \Phi(\eta_0)$ nicht durch q theilbar sein kann. Diese Resultate können wir nach der vorigen Nummer auch so aussprechen: Die reellen Zahlen $F(u_i)$ und $\Phi(u_i)$ sind durch q nicht theilbar. Wäre nun

$$\psi(\eta_k) \,.\, f(r) \,.\, \varphi(r) \equiv 0 \pmod{q},$$

so müsste umsomehr auch

$$\psi(\eta_k) \,.\, F(\eta_0) \,.\, \Phi(\eta_0) \equiv 0 \pmod{q}$$

sein, was gleichbedeutend ist mit der Folgerung, dass das Product $F(u_i) \,.\, \Phi(u_i)$ zweier reeller Zahlen, welche, wie soeben gezeigt, den Primfactor q nicht enthalten, durch diesen Factor theilbar sein müsste, also absurd ist.

2) Hat die complexe Zahl $f(r)$ den zur Substitution $\binom{\eta_{k+k}}{u_h}$ gehörigen idealen Primfactor von q genau m mal, die complexe Zahl $\varphi(r)$ denselben Primfactor genau n mal, so enthält ihn das entwickelte Product beider genau $m+n$ mal. In der That, die Voraussetzungen werden durch folgende Congruenzbedingungen ausgesprochen:

$\psi(\eta_k)^m . f(r) \equiv 0 \pmod{q^m}$ aber nicht mehr $\psi(\eta_k)^{m+1} . f(r) \equiv 0 \pmod{q^{m+1}}$
$\psi(\eta_k)^n . \varphi(r) \equiv 0 \pmod{q^n}$ aber nicht mehr $\psi(\eta_k)^{n+1} . \varphi(r) \equiv 0 \pmod{q^{n+1}}$.

Man kann daher, indem $F(r)$, $\Phi(r)$ gewisse ganze complexe Zahlen bezeichnen,

$$\psi(\eta_k)^m . f(r) = q^m . F(r), \quad \psi(\eta_k)^n . \varphi(r) = q^n . \Phi(r)$$

setzen, woraus folgt

$$\psi(\eta_k)^{m+1} . f(r) = q^m . \psi(\eta_k) F(r), \quad \psi(\eta_k)^{n+1} . \varphi(r) = q^n . \psi(\eta_k) \Phi(r),$$

während weder $\psi(\eta_k) . F(r)$ noch $\psi(\eta_k) . \Phi(r)$ durch q theilbar sein darf. Nach dem vorigen Satze kann demnach auch $\psi(\eta_k) . F(r) \Phi(r)$ nicht durch q theilbar, also

$$\psi(\eta_k)^{m+n+1} . f(r) \varphi(r) = q^{m+n} . \psi(\eta_k) F(r) \Phi(r)$$

nicht durch q^{m+n+1} theilbar sein; da andererseits

$$\psi(\eta_k)^{m+n} . f(r) \varphi(r) = q^{m+n} . F(r) \Phi(r)$$

durch q^{m+n} theilbar ist, so ergiebt sich das Resultat:

zwar ist $\psi(\eta_k)^{m+n} . f(r) \varphi(r) \equiv 0 \pmod{q^{m+n}}$ aber nicht mehr
$$\psi(\eta_k)^{m+n+1} . f(r) \varphi(r) \equiv 0 \pmod{q^{m+n+1}}$$

welches den zu beweisenden Satz ausspricht.

3) Wenn eine complexe Zahl $F(r)$ alle idealen Primfactoren der Primzahl q mindestens m Mal enthält, so ist sie durch q^m theilbar. In der That, der Voraussetzung gemäss besteht die Congruenz (19) für alle Werthe von k, also das folgende System von Congruenzen:

$$\psi(\eta_0)^m . F(r) \equiv 0, \; \psi(\eta_1)^m . F(r) \equiv 0, \ldots \psi(\eta_{e-1})^m . F(r) \equiv 0 \pmod{q^m},$$

aus welchen

$$(20) \quad [\psi(\eta_0)^m + \psi(\eta_1)^m + \ldots + \psi(\eta_{e-1})^m] . F(r) \equiv 0 \pmod{q^m}$$

hervorgeht. Nun ist die in der Klammer stehende Grösse als ganze und ganzzahlige symmetrische Function der Perioden eine ganze reelle Zahl, von welcher man leicht nachweist, dass sie durch q nicht theilbar ist. Denn diese Theilbarkeit würde nicht aufhören, wenn man mit $\psi(\eta_0)^{q^n - m}$ multiplicirte, in welcher Potenz $q^n > m$ gewählt sein soll; da aber das Product zweier ψ-Functionen stets durch q theilbar ist, würde man so das Resultat

$$\psi(\eta_0)^{q^n} \equiv 0 \pmod{q}$$

oder nach (11) einfacher $\psi(\eta_0) \equiv 0 \pmod{q}$ erhalten, was nicht der Fall ist. Demnach kann man in der Congruenz (20) den

Factor von $F(r)$ unterdrücken und findet:

$$F(r) \equiv 0 \pmod{q^m}.$$

4) Wenn eine complexe Zahl $F(r)$ genau m ideale Primfactoren von q enthält, gleichviel, ob sie einzelne dieser Factoren mehrfach, oder lauter verschiedene derselben enthält, so ist ihre vollständige Norm durch q^{mf} theilbar. Zum Beweise dieses Satzes bemerken wir zunächst, dass, wenn $F(r)$ den zur Substitution $\binom{\eta_{h+k}}{u_h}$ gehörigen idealen Primfactor von q n Mal enthält, die conjugirte Zahl $F(r^g)$ den zur Substitution $\binom{\eta_{h+k+1}}{u_h}$ gehörigen idealen Primfactor des q ebenfalls n Mal enthält, denn aus der Congruenz

$$\psi(\eta_k)^n \,.\, F(r) \equiv 0 \pmod{q^n},$$

welche als Gleichung auch so geschrieben werden kann:

$$\psi(\eta_k)^n \,.\, F(r) = q^n \,.\, \Psi(r),$$

ergiebt sich durch Vertauschung von r mit r^g die nachstehende Gleichung

$$\psi(\eta_{k+1})^n \,.\, F(r^g) = q^n \,.\, \Psi(r^g)$$

oder die Congruenz

$$\psi(\eta_{k+1})^n \,.\, F(r^g) \equiv 0 \pmod{q^n},$$

welche das Behauptete beweist. Da hiernach je e successive Factoren der vollständigen Norm $\mathrm{N}F(r)$ jeden idealen Primfactor von q ebensooft enthalten, als der erste Factor $F(r)$ einen bestimmten derselben enthält, muss das Product von je e successiven Factoren der Norm nach dem vorigen Satze durch q^m, die Norm selbst also durch q^{mf} theilbar sein, wenn $F(r)$ überhaupt m ideale Primfactoren von q enthält.

9. Ehe wir in der Reihe dieser Sätze weiter fortfahren, müssen wir noch eine Ergänzung hier einschalten, die Primfactoren unserer complexen Zahlentheorie betreffend. Bisher ist nur von den von p verschiedenen reellen Primzahlen und ihrer Zerlegung in wirkliche oder allgemeiner in ideale Primfactoren die Rede gewesen, die Frage also offen geblieben, wie p selbst sich zu solcher Zerlegung verhalte.

Zunächst findet man sehr leicht, dass p in $p - 1$ complexe Factoren zerlegbar ist. Denn, setzt man in der identischen Gleichung

$x^{p-1}+x^{p-2}+\ldots+x+1=(x-r)(x-r^2)\ldots(x-r^{p-1})$
$x=1$, so findet man

$$p=(1-r)(1-r^2)\ldots(1-r^{p-1}).$$

Betrachten wir nun zwei dieser Factoren, z. B. $1-r$ und $1-r^n$; da der Quotient Beider gleich $1+r+r^2+\ldots+r^{n-1}$ ist, so ist er eine ganze complexe Zahl. Diese ist aber offenbar eine complexe Einheit, denn ihre Norm:

$$\frac{(1-r^n(1-r^{2n})\ldots(1-r^{(p-1)n})}{(1-r)(1-r^2)\ldots(1-r^{p-1})}$$

hat den Werth Eins. Bezeichnet man daher den Quotienten mit $E(r)$, so findet man

$$1-r^n=E(r)\,.\,(1-r)$$

d. h. den Satz: die Primzahl p ist in $p-1$ complexe Factoren zerlegbar, welche abgesehen von Einheiten, durch welche sie multiplicirt sind, sich nicht von einander unterscheiden.

Jeder dieser Factoren ist ein Primfactor; denn, wäre z. B. $1-r^n$ in die beiden Factoren $f(r)$, $\varphi(r)$ zerlegbar, welche von Einheiten verschieden sind, so müsste

$$p=\mathrm{N}(1-r^n)=\mathrm{N}f(r)\,.\,\mathrm{N}\varphi(r),$$

also etwa $\mathrm{N}f(r)=p$, $\mathrm{N}\varphi(r)=1$ d. h. $\varphi(r)$ eine Einheit sein, gegen die Voraussetzung.

Hiernach enthält die Primzahl p nur einen einzigen complexen Primfactor $1-r$, von welchem die übrigen nicht wesentlich verschieden sind, und es ist daher hier nie die Frage, welchen Primfactor von p eine gegebene complexe Zahl enthalte, sondern immer nur, wieviele? Letztere Frage aber ist leicht zu entscheiden. Dazu beweisen wir noch den Satz: Das Product zweier Zahlen $f(r)$, $\varphi(r)$ kann nur dann durch $1-r$ theilbar sein, wenn es einer der Factoren ist. In der That, da offenbar

$$(A_1 r+A_2 r^2+\ldots+A_{p-1}r^{p-1})^p\equiv A_1+A_2+\ldots+A_{p-1}\ (\text{mod. }p)$$

ist, weil $r^p=1$ und nach Fermat's Satze $A_i^p\equiv A_i$ (mod. p) ist, so wird auch in Beziehung auf den Modulus $1-r$

$$f(r)^p\equiv f(1),\ \varphi(r)^p\equiv\varphi(1)$$

sein, folglich, wenn die Congruenz

$$f(r) \cdot \varphi(r) \equiv 0 \text{ mod. } (1 - r)$$

stattfindet, durch Erhebung zur p^{ten} Potenz sich auch die folgende ergeben:

$$f(1) \cdot \varphi(1) \equiv 0 \text{ mod. } (1 - r).$$

Da aber eine reelle Zahl, wenn sie durch $1 - r$ theilbar ist, offenbar auch durch p theilbar sein muss, so wird $f(1) \cdot \varphi(1)$ also etwa $f(1)$ durch p und deshalb durch $1 - r$ theilbar sein, was die Congruenz

$$f(1) \equiv 0 \text{ mod. } (1 - r)$$

und, da $f(1) - f(r)$ algebraisch durch $1 - r$ theilbar ist,

$$f(r) \equiv 0 \text{ mod. } (1 - r)$$

liefert, wie bewiesen werden sollte.

Dieser Satz lehrt nun, dass zur Entscheidung der Frage, wieoft eine complexe Zahl $F(r)$ den Primfactor $1 - r$ enthalte, es hinreicht, sooft mit $1 - r$ in $F(r)$ algebraisch zu dividiren, als es sich möglich erweist. Ergiebt sich dabei, dass $F(r)$ den Factor $1 - r$ genau n Mal enthält, so muss die vollständige Norm $NF(r)$ den Primfactor p auch genau n Mal enthalten.

10. Das zuletzt erhaltene Ergebniss, verbunden mit dem Schlusssatze der Nr. 8 führt nun zu der wichtigen Folgerung, dass jede complexe Zahl nur eine endliche Anzahl idealer Primfactoren enthalten kann. Denn die vollständige Norm jeder solchen Zahl ist nothwendig eine endliche reelle ganze Zahl, die nur eine beschränkte Anzahl reeller Primfactoren in sich enthalten kann. Jene Sätze aber sagen aus, dass die Norm durch p^n theilbar ist, wenn die complexe Zahl n Factoren des p, durch q^{mf}, wenn sie m ideale Primfactoren der zum Exponenten f (mod. p) gehörigen Primzahl q, durch $q^{m'f'}$, wenn sie m' ideale Primfactoren der zum Exponenten f' (mod. p) gehörigen Primzahl q', u. s. w. enthält; eine unbeschränkte Anzahl idealer Primfactoren der complexen Zahl würde also mit Nothwendigkeit eine unbeschränkte Anzahl reeller Primfactoren der Norm zur Folge haben, wodurch die Richtigkeit des ausgesprochenen Satzes erhellt.

Ist nun eine complexe Zahl $F(r)$ gegeben, so zeigt die Zerlegung ihrer Norm in reelle Primfactoren sogleich an, von welchen Primzahlen überhaupt nur ideale Primfactoren in $F(r)$ enthalten

sein können, und nachdem man für diese die Functionen ψ gebildet hat, dienen dieselben zur Entscheidung, welche der idealen Primfactoren der in $\mathrm{N}F(r)$ enthaltenen Primzahlen, und wie oft ein jeder in $F(r)$ vorkomme. Diese Fragen sind demnach völlig bestimmt, wenn die complexe Zahl $F(r)$ gegeben ist, ein Resultat, welches das Analogon zu dem Hauptsatze der reellen Zahlentheorie ist, nach welchem jede Zahl sich nur auf eine Weise als Product von Primzahlen darstellen lässt.

Fragen wir nun auch umgekehrt, ob durch Angabe sämmtlicher idealer Primfactoren, der gleichen wie der verschiedenen, welche in einer complexen Zahl enthalten sein sollen, diese selbst völlig bestimmt sei, oder inwieweit eine Unbestimmtheit zurückbleibe. Nehmen wir also an, zwei complexe Zahlen $F(r)$ und $\Phi(r)$ enthalten genau dieselben idealen Primfactoren, nämlich den Factor $1 - r$ genau n Mal, einen idealen Primfactor der zu f gehörigen Primzahl q genau m Mal u. s. w. Dann werden auch die beiden Zahlen

$$\Phi(r) \,.\, F(r^g) \,.\,.\,.\,.\, F(r^{g^{p-2}})$$

und

$$F(r) \,.\, F(r^g) \,.\,.\,.\,.\, F(r^{g^{p-2}}) = \mathrm{N}F(r)$$

genau dieselben Primfactoren enthalten. Da aber die letztere gleich dem Producte der Zahlen p^n, q^{mf}, ... ist, muss die erstere durch das Product derselben theilbar sein, also der Quotient

$$\frac{\Phi(r) \,.\, F(r^g) \,.\,.\,.\,.\, F(r^{g^{p-2}})}{\mathrm{N}F(r)} = \frac{\Phi(r)}{F(r)} = E(r)$$

eine ganze complexe Zahl sein. Aus dieser Gleichung folgt aber

$$\Phi(r) = F(r) \,.\, E(r)$$

und durch den Uebergang zu den Normen und, wenn man die Gleichheit der beiden Normen $\mathrm{N}\Phi(r)$ und $\mathrm{N}F(r)$ bedenkt, die Gleichung:

$$\mathrm{N}E(r) = 1$$

d. h. $E(r)$ ist eine complexe Einheit.

So ergiebt sich als Antwort auf die genannte Frage folgender Satz:

Zwei complexe Zahlen, welche die nämlichen idealen Primfactoren enthalten, unterscheiden sich

von einander nur um eine Einheit, die als Factor hinzutreten kann. —

Bisher ist die, auf ihre idealen Primfactoren hin zu untersuchende complexe Zahl stets als eine wirkliche angenommen worden. Es ist aber klar, dass, wenn man einen Complex von irgend welchen idealen Primfactoren d. h. die sie definirenden Congruenzbedingungen beliebig giebt, diesen nicht stets eine wirklich existirende complexe Zahl zu entsprechen braucht, sondern dass dadurch im Allgemeinen eine nur ideale Zahl definirt sein wird. Hiervon wäre nun zunächst zu handeln. Jedoch werden wir darauf hier nicht mehr eingehen, da es, wie bemerkt, nicht von uns beabsichtigt wird, die gesammte Theorie der complexen Zahlen darzustellen, vielmehr nur soviel von derselben auseinanderzusetzen, als zum Verständniss der Anwendung, welche wir auf die Kreistheilung davon machen werden, nothwendig ist. Da wir es dabei aber nur mit wirklichen complexen Zahlen zu thun haben werden, so reicht das in dieser Vorlesung Mitgetheilte vollständig aus.

Neunzehnte Vorlesung.

Anwendung der Theorie der complexen Zahlen auf die Kreistheilung.

1. Indem wir uns nunmehr der beabsichtigten Anwendung zuwenden, wollen wir, um den Gang der Untersuchung nicht zu unterbrechen, folgenden Hilfssatz vorher beweisen: Ist $F(r)$ eine complexe Zahl, welche der Bedingung

$$F(r) \,.\, F(r^{-1}) = 1$$

genügt, so muss sie gleich einer positiven oder negativen Potenz von r, gleich $\pm r^h$ sein. Wir wollen uns $F(r)$ auf die Form

$$F(r) = a_0 + a_1 r + a_2 r^2 + \ldots . + a_{p-1} r^{p-1}$$

gebracht denken, in welcher zwar die Coëfficienten nicht völlig bestimmt sind, da man, ohne den Werth der Function zu ändern, beliebig oft den Ausdruck

$$0 = 1 + r + r^2 + \ldots . + r^{p-1}$$

addiren oder subtrahiren kann, wo man aber deswegen gerade die Coëfficienten so gewählt denken kann, dass ihre Summe numerisch nicht grösser als $\frac{p-1}{2}$ wird. Denn, wäre dies in jener Form noch nicht der Fall, vielmehr

$$a_0 + a_1 + a_2 + \ldots + a_{p-1} = z \,.\, p + \alpha,$$

während α numerisch nicht grösser als $\frac{p-1}{2}$ ist, so brauchte man nur

$$z\,(1 + r + r^2 + \ldots + r^{p-1})$$

von ihr zu subtrahiren, und erhielte eine neue ähnliche Form, in welcher offenbar die Summe der Coëfficienten gleich α wäre. Nehmen wir also gleich von vornherein

$$-\frac{p-1}{2} \lesseqgtr a_0 + a_1 + \ldots + a_{p-1} \lesseqgtr + \frac{p-1}{2}$$

an.

Wenn man nun den Ausdruck $F(r)$ mit dem folgenden multiplicirt:

$$F(r^{-1}) = a_0 + a_1 r^{p-1} + a_2 r^{p-2} + \ldots + a_{p-1} r^1,$$

so findet man

$$F(r) \,.\, F(r^{-1}) = A_0 + A_1 r + \ldots + A_{p-1} r^{p-1},$$

wenn

$$\begin{aligned} A_0 &= a_0^2 + a_1^2 + a_2^2 + \ldots + a_{p-1}^2 \\ A_1 &= a_0 a_1 + a_1 a_2 + \ldots + a_{p-1} a_0 \\ A_2 &= a_0 a_2 + a_1 a_3 + \ldots + a_{p-1} a_1 \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

gesetzt wird. Da nun jeder der Factoren $F(r)$, $F(r^{-1})$ aus

$$a_0 + a_1 + a_2 + \ldots + a_{p-1}$$

Termen besteht, wenn man a_0 als Summe von a_0 Einheiten, $a_1 r$ als Summe von a_1 Gliedern r u. s. w. ansieht, so muss ihr Product, welches

$$A_0 + A_1 + A_2 + \ldots + A_{p-1}$$

Terme enthält,

$$(a_0 + a_1 + a_2 + \ldots + a_{p-1})^2$$

Glieder enthalten, oder es ist

$$(1) \quad A_0 + A_1 + \ldots + A_{p-1} = (a_0 + a_1 + \ldots + a_{p-1})^2.$$

Nach der Voraussetzung ist aber

$$A_0 + A_1 r + \ldots + A_{p-1} r^{p-1} = 1$$

oder auch

$$A_0 - A_{p-1} - 1 + (A_1 - A_{p-1}) r + \dots + (A_{p-2} - A_{p-1}) r^{p-2} = 0,$$

woraus wegen der Irreductibilität der Kreistheilungsgleichung sich für die Coëfficienten $A_1, A_2, \dots A_{p-1}$ ein gemeinschaftlicher Werth, welcher A heisse, für A_0 aber der Werth $A + 1$ ergiebt, sodass die Gleichung (1) die Gestalt

$$pA + 1 = (a_0 + a_1 + \dots a_{p-1})^2$$

annimmt und die Congruenz

$$(a_0 + a_1 + \dots + a_{p-1})^2 \equiv 1 \text{ (mod. } p)$$

also, da die Summe der Coëfficienten zwischen $+\frac{p-1}{2}$ und $-\frac{p-1}{2}$, inclusive der Grenzen, enthalten ist, die Gleichung

$$a_0 + a_1 + \dots + a_{p-1} = \pm 1$$

daher $A = 0$ und $A_0 = 1$ liefert. Diese Gleichung kann aber, da A_0 die Summe von p Quadratzahlen ist, nicht anders bestehen, als wenn $p - 1$ dieser Zahlen gleich Null, die übrige gleich Eins ist, wodurch aber die complexe Zahl $F(r)$ sich auf ein einziges Glied von der Form $\pm r^h$ reducirt.

2. Um nun zu unserm Gegenstande überzugehen, wollen wir uns an die Methode erinnern, welche in der 8. Vorlesung zur Auflösung der Kreistheilungsgleichung mitgetheilt worden ist, und wesentlich darauf hinauslief, die Ausdrücke, welche dort mit (ω^h, r) bezeichnet wurden, und aus denen die Wurzeln der Kreistheilungsgleichung leicht zusammengesetzt werden können, zu finden. Wir werden hier in die eigentliche Natur dieser Ausdrücke von dem Standpunkte der complexen Zahlentheorie aus tiefer einzudringen versuchen. Doch müssen wir, um uns an die Bezeichnungen der vorhergehenden Vorlesung anlehnen zu können, die früher gebrauchte etwas verändern.

Es sei p eine Primzahl und r eine primitive Wurzel der Gleichung $x^p = 1$, q sei ebenfalls eine Primzahl, von der Form $\mu p + 1$, und R eine primitive Wurzel der Gleichung $x^q = 1$, unter ω verstehen wir eine primitive Wurzel der Gleichung $x^{q-1} = 1$, sodass wir $r = \omega^{-\mu}$ setzen dürfen, endlich sei γ eine primitive Wurzel (mod. q). Wenn man dann setzt:

$$(\omega, R) = R + \omega \,.\, R^{\gamma} + \omega^2 \,.\, R^{\gamma^2} + \dots + \omega^{q-2} \,.\, R^{\gamma^{q-2}},$$

so ist nach (28) und (30) der 8. Vorlesung der Ausdruck

$$\psi_k(r) = \frac{(r,R).(r^k,R)}{(r^{k+1},R)} = \frac{(\omega^{-\mu},R)(\omega^{-k\mu},R)}{(\omega^{-(k+1)\mu},R)},$$

wenn $k+1$ nicht durch p theilbar ist, eine ganze Function von r allein mit ganzzahligen Coëfficienten, also eine ganze, aus r gebildete complexe Zahl. Setzt man ausserdem

$$\psi(q-1-m,\ q-1-n,\ \omega) = \frac{(\omega^{q-1-m},R)(\omega^{q-1-n},R)}{(\omega^{2(q-1)-m-n},R)}$$

und ersetzt darin ω durch γ, so ist nach Nr. 2 der 10. Vorlesung

$$\psi(q-1-m,\ q-1-n,\ \gamma) \equiv 0 \pmod{q},$$

wenn m, n positive ganze Zahlen bedeuten, die zwar selbst kleiner als $q-1$ sind, deren Summe aber $q-1$ übersteigt.

Andererseits hat, da q eine (mod. p) zum Exponenten 1 gehörige Primzahl ist, nach dem ersten Satze in Nr. 4 der 17. Vorlesung die Congruenz

$$x^{p-1} + x^{p-2} + \ldots + x + 1 \equiv 0 \pmod{q}$$

$p-1$ reelle Wurzeln, welche leicht anzugeben, nämlich durch die Potenzen

$$\gamma^{-\mu},\ \gamma^{-2\mu},\ \ldots\ \gamma^{-(p-1)\mu}$$

dargestellt sind. In der That sind diese Werthe (mod. q) incongruent und ein beliebiger derselben: $\gamma^{-h\mu}$ leistet der Congruenz Genüge, da $p\mu = q-1$, also $\frac{\gamma^{-ph\mu}-1}{\gamma^{-h\mu}-1} \equiv 0 \pmod{q}$ ist. Zur Abkürzung setzen wir $\gamma^{-\mu} = u$.

Nun sind die Wurzeln dieser Congruenz aber den Wurzeln der Gleichung

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$$

zugeordnet, und zwar ist leicht zu sehen, dass, wenn wir u dem r zuordnen, allgemein u^h und r^h zugeordnete Congruenz- und Gleichungswurzeln sein werden. Denn, bezeichnet man r^h mit r', so muss, (nach dem Hauptsatze in Nr. 6 der 17. Vorlesung) die Gleichung $r' = r^h$ in eine richtige Congruenz (mod. q) übergehen, wenn man die Gleichungswurzeln durch die entsprechenden Congruenzwurzeln ersetzt; die, r' entsprechende Congruenzwurzel u' leistet also der Bedingung $u' \equiv u^h \pmod{q}$ Genüge, wie behauptet.

Dies vorausgeschickt, können wir die idealen Primfactoren von q characterisiren. Da die Primzahl q zum Exponenten 1

(mod. p) gehört, zerfällt sie in $p-1$ ideale Primfactoren, von denen $f(r)$ der zur Substitution $\binom{r}{u}$ gehörige sein möge; dann ist $f(r^h)$ der zur Substitution $\binom{r^h}{u}$, oder auch, wenn m_h so bestimmt wird, dass $h \, . \, m_h \equiv 1$ (mod. p) ist, der zur Substitution $\binom{r}{u^{m_h}}$ gehörige ideale Primfactor von q.

3. Wir setzen nun in der Function ψ für m den Werth $h \, . \, \mu$, und wählen $n \equiv km$ mod. $(q-1)$, wodurch offenbar auch n als Vielfaches von μ bestimmt wird, da m und $q-1 = p\mu$ diesen Factor gemeinsam haben. Da m zwischen den Grenzen 0 und $q-1$ liegen soll, so kann h einen der Werthe $1, 2, 3, \ldots p-1$ haben, und dasselbe folgt für k, da wegen $\frac{n}{\mu} \equiv kh$ (mod. p) für alle Werthe des h aus jener Reihe der Werth des k eben diese Reihe durchläuft. — Weil n den kleinsten positiven Rest von km mod. $(q-1)$ bedeutet, so muss, wie leicht zu übersehen, $\frac{n}{\mu}$ der kleinste positive Rest von kh (mod. p) sein; werden demnach m und n so gewählt, dass $m+n > q-1$ ist, so kann Dies, indem durch μ dividirt wird, auch so ausgedrückt werden, dass die Summe von h und dem kleinsten positiven Reste von kh (mod. p) grösser als p sein solle.

Nach diesen Vorbemerkungen sehen wir nun zu, was aus $\psi(q-1-m, q-1-n, \omega)$ bei den gewählten Werthen von m und n hervorgeht. Man findet aber

$$\psi(q-1-h\mu, q-1-kh\mu, \omega) = \frac{(\omega^{-h\mu}, R) . (\omega^{-kh\mu}, R)}{(\omega^{-(k+1)h\mu}, R)} = \psi_k(\omega^{-h\mu}) = \psi_k(r^h).$$

Aehnlicherweise wird sich

$$\psi(q-1-h\mu, q-1-kh\mu, \gamma) \equiv \psi_k(u^h) \text{ (mod. } q)$$

ergeben, und weil $m+n > q-1$ ist,

$$\psi_k(u^h) \equiv 0 \text{ (mod. } q).$$

Dies wird in Worten folgendermassen ausgedrückt: Die complexe Zahl $\psi_k(r)$ wird durch q theilbar, wenn r durch die Congruenzwurzel u^h ersetzt wird, oder auch: sie enthält den zur Substitution $\binom{r}{u^h}$ gehörigen idealen Primfactor des q jedesmal, wenn die Summe aus h

und dem kleinsten positiven Reste von kh (mod. p) grösser als p ist.

Hieraus ergiebt sich mit Leichtigkeit die Zerlegung von $\psi_k(r)$ in ideale Primfactoren. Bemerken wir vor Allem, dass von je zwei Werthen des h, welche die Summe p haben, stets ein einziger der Bedingung genügt; dass h und der kleinste positive Rest von kh (mod. p) eine grössere Summe geben als p. In der That, sei y der kleinste positive Rest von kh (mod. p), so ist $p - y$ der kleinste positive Rest von $k(p - h)$ (mod. p); denn, setzt man $kh = pz + y$, so folgt $(p - h)k = p(k - z - 1) + (p - y)$. Ferner folgt aus der Ungleichheit $h + y \gtrless p$ stets die andere:

$$2p - (h + y) = (p - h) + (p - y) \lessgtr p,$$

womit die Behauptung erwiesen ist.

Da es hiernach für jedes bestimmte k genau $\frac{p-1}{2}$ Werthe des h von der angegebenen Beschaffenheit giebt, so folgt unmittelbar, dass $\psi_k(r)$ ebensoviel verschiedene ideale Primfactoren von q, jeden mindestens einmal, enthalten muss. Andere Primfactoren, als solche von q, kann $\psi_k(r)$ aber nicht enthalten, da aus der Formel (2) der 10. Vorlesung, wenn q statt p, μ statt h, $k\mu$ statt k gesetzt wird, die Gleichung

$$\psi_k(r) \cdot \psi_k(r^{-1}) = q \tag{2}$$

hervorgeht. Diese lehrt ferner, dass $\psi_k(r)$ jeden idealen Primfactor auch nur einmal enthalten kann, da Gleiches bei q stattfindet; endlich, weil die conjugirte Zahl $\psi_k(r^{-1})$ offenbar genau soviel ideale Primfactoren enthalten muss, als $\psi_k(r)$, Beide zusammen aber nur ebensoviel haben können, als q, welches deren $p - 1$ hat, so kann $\psi_k(r)$ überhaupt nicht mehr, als jene $\frac{p-1}{2}$ ideale Primfactoren enthalten.

Da nun mit $f(r)$ der zur Substitution $\binom{r}{u}$ gehörige ideale Primfactor von q bezeichnet worden ist, so ist $f(r^{m_h})$ der zur Substitution $\binom{r}{u^h}$ gehörige, wenn m_h als kleinste positive Zahl, für welche $h \,.\, m_h \equiv 1$ (mod. p) ist, gewählt wird. Demnach ent-

hält $\psi_k(r)$ alle diejenigen Primfactoren $f(r^{m^h})$, bei denen h und der kleinste positive Rest von kh (mod. p) eine grössere Summe geben, als p. Nach dem Schlussatze der letzten Vorlesung ist also:

$$\psi_k(r) = E(r) \cdot \prod f(r^{m^h}),$$

wo das Product über die $\frac{p-1}{2}$ bezeichneten Werthe des h zu beziehen, und $E(r)$ eine complexe Einheit ist. Ebenso ist

$$\psi_k(r^{-1}) = E(r^{-1}) \cdot \prod f(r^{m^h})$$

wo das Product auf die $\frac{p-1}{2}$ übrigen Werthe des h zu beziehen ist. Der Gleichung (2) wegen, und, weil das Product aller idealen Primfactoren des q gleich dieser Zahl ist, findet man leicht die Bedingung

$$E(r) \cdot E(r^{-1}) = 1,$$

woraus nach dem Hilfssatze in Nr. 1 sich $E(r) = \pm r^n$ ergiebt. Endlich wird also:

$$\psi_k(r) = \pm r^n \cdot \prod f(r^{m^h}) \,. \tag{3}$$

4. Nachdem auf diese Weise $\psi_k(r)$ bestimmt worden ist, findet man auch leicht den Werth des, bei der Berechnung der Wurzeln der Gleichung $x^q = 1$ auftretenden Ausdruckes $(\omega^{-\mu}, R) = (r, R)$. Denn die Formel (34) der 8. Vorlesung, in die hier angenommene Bezeichnung übertragen, liefert folgende Gleichung:

$$(r, R)^p = (-1)^\mu \cdot q \cdot \psi_1(r)\, \psi_2(r) \ldots \psi_{p-2}(r). \tag{4}$$

Nehmen wir nun den bestimmten idealen Primfactor $f(r^{m^h})$ von q, welcher zur Substitution $\binom{r}{u^h}$ gehört, so ist dieser in jeder der Functionen $\psi_k(r)$ enthalten, deren k der Bedingung genügt, dass h und der kleinste positive Rest von kh (mod. p) eine grössere Summe als p haben, oder für welche der kleinste positive Rest von kh (mod. p) grösser als $p-h$ ist. Den im Producte (4) auftretenden Werthen $1, 2, 3, \ldots p-2$ des k entsprechen aber als kleinste positive Reste von kh die Werthe $1, 2, 3, \ldots p-1$ mit Ausnahme von $p-h$, da aus der Congruenz $kh \equiv p-h$ (mod. p) sich $(k+1)\,h \equiv 0$ oder $k \equiv p-1$ (mod. p) ergeben würde. Unter diesen Resten des kh sind daher $h-1$ grösser als $p-h$, folglich kommt der zur Substitution

$\left(\frac{r}{u^h}\right)$ gehörige Primfactor des q in dem Producte der ψ-Functionen genau $h - 1$ Mal, und da er noch einmal in q enthalten ist, im ganzen Producte genau h Mal vor. Da hierdurch die idealen Primfactoren von $(r, R)^p$ vollständig definirt sind, ist dieser Ausdruck bis auf eine Einheit wieder völlig bekannt, nämlich offenbar

$$(r, R)^p = E(r) \, . \, f(r^{m_1})^1 \, . \, f(r^{m_2})^2 \ldots f(r^{m_{p-1}})^{p-1}.$$

Dafür kann man auch schreiben:

$$(r, R)^p = E(r) \, . \, f(r)^{m_1} \, . \, f(r^2)^{m_2} \ldots . f(r^{p-1})^{m_{p-1}}.$$

Die Einheit muss aber wieder gleich $\pm r^m$ sein, denn nach Gleichung (4) findet man mit Rücksicht auf die Gleichung (2)

$$(r, R)^p \, . \, (r^{-1}, R)^p = q^p;$$

nach der vorigen Gleichung aber erhält dies Product den Werth

$$E(r) \, . \, E(r^{-1}) \, . \, q^p,$$

wenn man beachtet, dass aus der Congruenz $h \, . \, m_h \equiv 1 \pmod{p}$ auch

$$(p - h) \, . \, (p - m_h) \equiv 1 \pmod{p}$$

und durch Vergleichung mit der andern: $(p - h) \, . \, m_{p-h} \equiv 1 \pmod{p}$ die Gleichung $m_{p-h} = p - m_h$ folgt, und wenn man ferner bemerkt, dass deshalb der Factor $f(r^{p-h})^{m_{p-h}}$ aus dem Producte $(r, R)^p$, mit dem Factor $f(r^{-h})^{m_h}$ aus dem Producte $(r^{-1}, R)^p$ multiplicirt,

$$f(r^{p-h})^{m_{p-h}+m_h} = f(r^{p-h})^p$$

liefert, demnach im Producte $(r, R)^p \, . \, (r^{-1}, R)^p$ alle idealen Primfactoren von q zur p^{ten} Potenz erhoben vorkommen. Die Vergleichung beider Werthe des Products $(r, R)^p \, . \, (r^{-1}, R)^p$ liefert die Gleichung

$$E(r) \, . \, E(r^{-1}) = 1$$

d. h. $E(r) = \pm r^m$. So findet man endlich

$$(5) \qquad (r, R)^p = \pm r^m \, . \, f(r)^{m_1} \, . \, f(r^2)^{m_2} \ldots . f(r^{p-1})^{m_{p-1}},$$

eine Gleichung, in welcher Alles bestimmt ist, bis auf den Factor $\pm r^m$. Aber auch dieser bestimmt sich mittels folgender Bemerkung: Erhebt man den Ausdruck

$$(r, R) = R + r \, . \, R^\gamma + r^2 \, . \, R^{\gamma^2} + \ldots . + r^{q-2} \, . \, R^{\gamma^{q-2}}$$

zur p^{ten} Potenz, so findet man nach dem polynomischen Lehr-

satze, und, weil $r^p = 1$ ist,

$$(r, R)^p \equiv R^p + R^{p\gamma} + R^{p\gamma^2} + \dots R^{p\gamma^{q-2}} \pmod{p}$$

d. h. congruent der Summe aller imaginären Wurzeln der Gleichung $R^q = 1$, welche den Werth -1 hat. Es muss also $\pm r^m$ so gewählt werden, dass die rechte Seite der Gleichung (5) ebenfalls diese Congruenzbedingung erfüllt.

5. Wir wollen diese Betrachtungen mit der numerischen Berechnung eines Beispieles beschliessen. Sei $p = 5$, $q = 11$, wo dann $\gamma = 2$ als primitive Wurzel genommen werden kann. Da $\mu = 2$ ist, findet man $\gamma^{-\mu} \equiv 3$, folglich entsprechen, wenn 3 als die, der Wurzel r zugeordnete Congruenzwurzel angesehen wird, den Wurzeln

$$r,\ r^2,\ r^3,\ r^4$$

die Congruenzwurzeln

$$3,\ 9,\ 5,\ 4\,.$$

Suchen wir nun zuerst eine complexe Zahl zu bestimmen, welche den, dieser Zuordnung entsprechenden idealen Primfactor von q enthält. Dazu sind nach Nr. 2 der letzten Vorlesung die Unbestimmten x_1, x_2, x_3, x_4 in dem Ausdrucke

$$x_1 r + x_2 r^2 + x_3 r^3 + x_4 r^4$$

so zu wählen, dass nach Substitution der Congruenzwurzeln statt der zugehörigen Perioden derselbe durch $q = 11$ theilbar, dass also die Congruenz

$$3x_1 + 9x_2 + 5x_3 + 4x_4 \equiv 0 \pmod{11}$$

erfüllt wird. Dies geschieht z. B., wenn $x_1 = 2$, $x_2 = 1$, $x_3 = x_4 = 2$ gesetzt wird, also ist

$$2r + r^2 + 2r^3 + 2r^4 = -2 - r^2$$

oder auch $2 + r^2$ eine complexe Zahl, welche den zur Substitution $\binom{r}{3}$ gehörigen idealen Primfactor von 11 enthält. Da man aber durch Ausrechnung des Productes findet, dass

$$N(2 + r^2) = (2 + r)(2 + r^2)(2 + r^3)(2 + r^4) = 11$$

ist, so ist diese Primzahl in wirkliche Primfactoren zerlegbar, und $2 + r^2$ der zur Substitution $\binom{r}{3}$ gehörige ideale, in diesem Falle aber zugleich auch wirkliche Primfactor von 11. Setzt man nun $f(r) = 2 + r^2$, so ist

$$f(r^2) = 2 + r^4,\ f(r^3) = 2 + r,\ f(r^4) = 2 + r^3,$$

und diese Primfactoren gehören zu den Substitutionen: $\binom{r^2}{3}$, $\binom{r^3}{3}$, $\binom{r^4}{3}$. Aber aus der Congruenz $h\ .\ m_h \equiv 1 \pmod{5}$ folgen, den Werthen $h = 1, 2, 3, 4$ entsprechend, die Werthe $m_h = 1, 3, 2, 4$, man kann daher die vier Primfactoren $2 + r^2$, $2 + r^4$, $2 + r$, $2 + r^3$ auch als die zu den Substitutionen $\binom{r}{3}$, $\binom{r}{3^3}$, $\binom{r}{3^2}$, $\binom{r}{3^4}$ gehörigen bezeichnen.

Die Formel (5) liefert sodann für $(r, R)^5$ folgenden Ausdruck:

$$(r, R)^5 = \pm r^m \,.\, (2 + r^2)\,(2 + r^4)^3\,(2 + r)^2\,(2 + r^3)^4,$$

in welchem nur noch der Factor $\pm r^m$ zu bestimmen bleibt. Das geschieht durch die Bemerkung, dass die Entwicklung des Products einen Ausdruck liefert, welcher $\equiv \mp r^{m+1} \pmod{5}$ gefunden wird; da er aber $\equiv -1 \pmod{5}$ sein muss, hat man das obere Zeichen und $m = 4$ zu wählen, und erhält so:

$$(r, R)^5 = + r^4\,(2 + r^2)\,(2 + r^4)^3\,(2 + r)^2\,(2 + r^3)^4. —$$

Die Entwicklung dieses Ausdrucks liefert, von der verschiedenen Bezeichnung abgesehen, wie es sein muss, den bereits in der 8. Vorlesung in Formel (48) gefundenen Werth von $(\alpha, \eta_0)^5$, mit welchem $(r, R)^5$ identisch wird, wenn α, r statt r, R geschrieben wird.

Durch die hier mitgetheilten Betrachtungen sind alle Elemente, deren man zur Auflösung der Gleichung $x^q = 1$ bedarf, auf die idealen Primfactoren der Zahl q zurückgeführt worden. Da die Wurzeln dieser Gleichung lediglich durch q selbst bedingt sein können, so hat man sie auf solche Weise durch diejenigen Grössen ausgedrückt, welche ihre wahren Elemente ausmachen, und in dieser Vollendung der Theorie beruht die Bedeutung der letzten Untersuchung, welche von Kummer in Crelle's Journal Bd. 35 (siehe auch Disputatio de num. complexis, in einer Gratulationsschrift der Breslauer Universität zur dritten Säcularfeier der Königsberger Universität, abgedruckt in Liouv. J. Bd. 12 unter dem Titel: „sur les nombres complexes, qui sont formés avec les nombres entiers réels et les racines de l'unité") zuerst veröffentlicht worden ist.

Zwanzigste Vorlesung.

Zwei Anwendungen auf die Theorie der quadratischen Formen.

1. In der 10. und 11. Vorlesung sind wir aus der Kreistheilung zu verschiedenen Darstellungen von Primzahlen durch quadratische Formen geführt worden. Den Ausgangspunkt der dortigen Betrachtungen bildete ein eigenthümliches Verhalten, welches die Resolvante zeigt, wenn die Einheitswurzel durch eine entsprechende Congruenzwurzel ersetzt wird, ein Verhalten, welches in dem Nr. 2 der 10. Vorlesung ausgesprochenen Satze seinen Ausdruck fand. Hier wollen wir zwei weitere Anwendungen der Kreistheilung auf die Theorie der quadratischen Formen zusammenstellen, von welchen die erste, auf Formen bezüglich, deren Determinante eine negative ungerade Primzahl $-p$ sein soll, auf einer Verallgemeinerung der in der angeführten Stelle gegebenen Betrachtungen beruht*), während die zweite sich auf Formen von einer positiven Determinante, welche eine ungerade Primzahl $+p$ ist, bezieht und an die in Nr. 3 der 15. Vorlesung gefundene Zerlegung von $4X$ in zwei quadratische Factoren anzuknüpfen ist.**)

Wir werden im Folgenden mit $\psi(h, k, \omega)$ oder kürzer mit $\psi(h, k)$ den Ausdruck

$$\frac{(\omega^{-h}, R).(\omega^{-k}, R)}{(\omega^{-h-k}, R)}$$

bezeichnen, in welchem

$$(\omega^{-h}, R) = \sum_{\lambda=1}^{\lambda=q-1} \omega^{-h\,\mathrm{ind.}\lambda}\,.\,R^{\lambda}$$

ist, während R eine primitive Wurzel der Gleichung $x^q = 1$, ω eine primitive Wurzel der Gleichung $x^{q-1} = 1$ bedeuten soll; p und q seien ungerade Primzahlen, welche in der durch die Gleichung $q = \mu p + 1$ ausgedrückten Beziehung stehen, und unter γ werde wieder eine primitive Wurzel (mod. q) verstanden.

*) Vgl. hierzu Smith, report on the theory of numbres, art. 121. Auch Jacobi's Note über Kreistheilung und Cauchy, mém. sur la th. des nombres, besonders die Noten II, III und XIII.

**) S. Dirichlet, sur la manière de résoudre l'équation $t^2 - pu^2 = 1$ au moyen des fonctions circulaires, Cr. J. Bd. 17. Desgl. Jacobi's Note.

Jener Ausdruck hat folgende Eigenschaften, die hier sogleich zusammengestellt werden sollen:

1) Ist $h' \equiv h$, $k' \equiv k$ (mod. $q-1$), so ist offenbar $\psi(h', k') = \psi(h, k)$.

2) Ist eine der beiden Zahlen h, k z. B. h gleich Null, so wird der entsprechende Ausdruck $(\omega^{-h}, R) = (1, R)$ d. i. der Summe

$$R + R^2 + \ldots + R^{q-1}$$

gleich, deren Werth -1 ist, der andere Ausdruck (ω^{-k}, R) dem Nenner (ω^{-h-k}, R) gleich, also ist $\psi(0, k) = -1$, ebenso $\psi(h, 0) = -1$. Dasselbe gilt aber offenbar auch, wenn h und k Beide verschwinden, da dann jede der Functionen in dem Ausdrucke den Werth -1 annimmt; man findet demnach auch noch $\psi(0,0) = -1$.

3) Wenn die Zahlen h, k nicht Null noch der Null mod. $(q-1)$ congruent sind und auch $h+k$ durch $q-1$ nicht theilbar ist, so wird nach Nr. 5 der 8. Vorlesung der Ausdruck

$$(1) \qquad \psi(h,k) = \frac{(\omega^{-h}, R) \cdot (\omega^{-k}, R)}{(\omega^{-h-k}, R)} = \sum_{\lambda=1}^{\lambda=q-2} \omega^{-h \operatorname{ind.} \lambda + (h+k) \operatorname{ind.} (1+\lambda)},$$

also einer ganzen Function von ω allein gleich. In diesem Falle ist bekanntlich

$$\psi(h,k) \cdot \psi(-h,-k) = \frac{(\omega^{h}, R)(\omega^{-h}, R) \cdot (\omega^{k}, R)(\omega^{-k}, R)}{(\omega^{h+k}, R)(\omega^{-h-k}, R)} = q$$

oder auch

$$(2) \qquad \psi(h,k) \cdot \psi(q-1-h, q-1-k) = q.$$

4) Ist $h+k$ durch $q-1$ theilbar, ohne dass h oder k es sind, so nimmt der Ausdruck $\psi(h,k)$, da $k \equiv -h$ mod. $(q-1)$ und der Nenner $(\omega^{h+k}, R) = -1$ wird, die Form $-(\omega^{h}, R)(\omega^{-h}, R)$ an, und wird nach Formel (29) der 8. Vorlesung gleich $-(-1)^{h} \cdot q$, folglich ist

$$(3) \qquad \psi(h,k) = (-1)^{h+1} \cdot q, \text{ wenn } h + k \equiv 0 \text{ mod. } (q-1).$$

2. Wir wollen nun unter $m_1, m_2, \ldots m_\alpha$ positive ganze Zahlen verstehen, welche kleiner als $q-1$ vorausgesetzt werden sollen, und das Product

$$(\omega^{-m_1}, R) \cdot (\omega^{-m_2}, R) \ldots (\omega^{-m_\alpha}, R)$$

bilden. Dies kann offenbar durch ψ-Functionen ausgedrückt werden; denn man erhält zuerst

$$(\omega^{-m_1}, R) \cdot (\omega^{-m_2}, R) = \psi(m_1, m_2) \cdot (\omega^{-(m_1+m_2)}, R),$$

sodann, wenn mit μ_2 der kleinste positive Rest von $m_1 + m_2$ mod. $(q - 1)$ bezeichnet wird, sodass $\mu_2 \equiv m_1 + m_2$ mod. $(q-1)$ ist,

$$(\omega^{-(m_1+m_2)}, R) \,.\, (\omega^{-m_3}, R) = \psi(\mu_2, m_3) \,.\, (\omega^{-(m_1+m_2+m_3)}, R),$$

ferner, wenn nun μ_3 den kleinsten positiven Rest von $m_1 + m_2 + m_3$ mod. $(q - 1)$ bezeichnet,

$$(\omega^{-(m_1+m_2+m_3)}, R) \,.\, (\omega^{-m_4}, R) = \psi(\mu_3, m_4) \,.\, (\omega^{-(m_1+m_2+m_3+m_4)}, R)$$

u. s. w., endlich, wenn $\mu_{\alpha-1}$ der kleinste positive Rest von

$$m_1 + m_2 + \dots + m_{\alpha-1} \text{ mod. } (q - 1)$$

ist,

$$(\omega^{-(m_1+m_2+\dots+m_{\alpha-1})}, R) \,.\, (\omega^{-m_\alpha}, R)$$
$$= \psi(\mu_{\alpha-1}, m_\alpha) \,.\, (\omega^{-(m_1+m_2+\dots+m_\alpha)}, R)\,.$$

Indem man alle diese Gleichungen in einander multiplicirt und die gemeinsamen Factoren beider Seiten weglässt, findet man folgende wichtige Formel:

$$(4)\quad (\omega^{-m_1}, R) . (\omega^{-m_2}, R) \dots (\omega^{-m_\alpha}, R) = \Psi(\omega) \,.\, (\omega^{-(m_1+m_2+\dots+m_\alpha)}, R),$$

in welcher

$$(5)\qquad \Psi(\omega) = \psi(m_1, m_2) \,.\, \psi(\mu_2, m_3) \dots \psi(\mu_{\alpha-1}, m_\alpha)$$

also eine ganze und ganzzahlige Function von ω allein ist, ebenso wie die Factoren aus denen es sich zusammensetzt. Betrachten wir nun diese Function etwas genauer.

Der allgemeine Factor $\psi(\mu_{i-1}, m_i)$ kann drei verschiedene Fälle darbieten, jenachdem

$$\mu_{i-1} + m_i = q - 1,\quad \mu_{i-1} + m_i > q - 1,\quad \mu_{i-1} + m_i < q - 1$$

ist. Im letzten lassen wir ihn ungeändert, im ersten ersetzen wir ihn nach Gleichung (3) durch seinen Werth $(-1)^{1+\mu_{i-1}} \,.\, q$, im zweiten schreiben wir dafür nach Gleichung (2)

$$\frac{q}{\psi(q - 1 - \mu_{i-1},\; q - 1 - m_i)},$$

in welchem Quotienten die ψ-Function des Nenners jetzt Argumente hat, die offenbar eine kleinere Summe ergeben, als $q - 1$.

Es entsteht die Frage, wieoft einer der beiden ersten Fälle eintreten wird. Da μ_{i-1} der kleinste positive Rest ist, welchen die Summe

$$m_1 + m_2 + \dots + m_{i-1}$$

durch $q - 1$ getheilt lässt, kann man

$$m_1 + m_2 + \dots + m_{i-1} = n_{i-1}(q-1) + \mu_{i-1}$$

setzen, indem man mit $n_{i-1}(q-1)$ das grösste, in der Summe enthaltene Vielfache von $(q-1)$ bezeichnet. Fügt man nun zu der Summe das folgende Glied m_i hinzu, und schreibt in analoger Weise

$$m_1 + m_2 + \dots + m_{i-1} + m_i = n_i(q-1) + \mu_i,$$

während nun $n_i(q-1)$ das grösste darin enthaltene Vielfache von $q-1$ ist, so sind zwei Fälle zu unterscheiden: entweder ist $\mu_{i-1} + m_i < q-1$, dann wird $n_i = n_{i-1}$ sein müssen; oder aber es ist $\mu_{i-1} + m_i \overline{>} q-1$, dann wird offenbar $n_i = n_{i-1} + 1$, da $\mu_{i-1} + m_i$ eine Summe zweier Zahlen ist, welche kleiner als $q-1$ sind, — die erste als kleinster positiver Rest mod. $(q-1)$, die zweite nach der Voraussetzung — deren Summe also jedenfalls $2(q-1)$ nicht erreichen kann. Hiernach wird sich das grösste, in der Summe

$$m_1 + m_2 + \dots + m_{i-1}$$

enthaltene Vielfache von $q-1$ durch Hinzufügen von m_i um eine Einheit vermehren oder constant bleiben, jenachdem von den drei, oben unterschiedenen Fällen einer der beiden ersten oder der letzte stattfindet. Wenn man daher annimmt, dass

$$m_1 + m_2 + \dots + m_\alpha = n_\alpha(q-1) + \mu_\alpha,$$

während $0 \overline{<} \mu_\alpha < q-1$ ist, so muss es genau n_α Mal geschehen, dass einer der beiden ersten Fälle eintritt.

Hiernach wird man bei Anwendung der angegebenen Transformationen des Factors $\psi(\mu_{i-1}, m_i)$

$$\Psi(\omega) = q^{n_\alpha} \cdot \frac{f(\omega)}{\varphi(\omega)} \tag{6}$$

finden, worin sowohl $f(\omega)$ als auch $\varphi(\omega)$ Producte aus solchen ψ-Functionen bedeuten, bei welchen die Argumente eine kleinere Summe geben als $q-1$.

3. Auf ψ-Functionen dieser Art lässt sich aber der Satz in Nr. 2 der 10. Vorlesung zur Anwendung bringen. Dabei unterscheiden wir wieder die drei früheren Fälle. Ist **erstens** $\mu_{i-1} + m_i = q-1$, so ist nach Gleichung (3):

$$\psi(\mu_{i-1}, m_i) = (-1)^{1+\mu_{i-1}} \cdot q = (-1)^{1+m_i} \cdot q;$$

in diesem Falle aber ist $\mu_i = 0$, und da man

$$1.2.3\dots m_i = (q-1-\mu_{i-1})(q-2-\mu_{i-1})\dots(q-m_i-\mu_{i-1})$$

also

$(-1)^{m_i}.1.2.3\ldots m_i \equiv (\mu_{i-1}+1)(\mu_{i-1}+2)\ldots(\mu_{i-1}+m_i) \pmod{q}$, folglich mit Rücksicht auf den Wilson'schen Satz

$$(-1)^{m_i}.\prod(m_i).\prod(\mu_{i-1}) \equiv 1.2.3\ldots(\mu_{i-1}+m_i) \equiv -1 \pmod{q}$$

findet, so kann man schreiben, wenn man in üblicher Weise übereinkommt, unter $\Pi(0)$ die Einheit zu verstehen,

$$(7) \qquad (-1)^{1+m_i} \equiv \frac{\Pi(\mu_i)}{\Pi(\mu_{i-1}).\Pi(m_i)} \pmod{q}.$$

Dass in dieser Congruenz ein Bruch auftritt, macht keine Schwierigkeit, da die Factoren des Nenners durch q nicht theilbar sind. Sooft nämlich A eine zu q relativ prime Zahl ist, kann man eine Zahl A' der Congruenz $AA' \equiv 1 \pmod{q}$ gemäss bestimmen, und unter dem Bruche $\frac{1}{A} \pmod{q}$ jede der Zahl $A' \pmod{q}$ congruente Zahl verstehen. In solcher Weise muss auch die vorige, sowie alle ähnlichen im Folgenden vorkommenden Congruenzen, welche Brüche enthalten, aufgefasst werden.

Ist zweitens $\mu_{i-1} + m_i > q - 1$, so wird nach dem Satze in Nr. 2 der 10. Vorlesung

$$\psi(q-1-\mu_{i-1}, q-1-m_i, \gamma) \equiv -\frac{\Pi(2q-2-\mu_{i-1}-m_i)}{\Pi(q-1-\mu_{i-1}).\Pi(q-1-m_i)} \pmod{q}$$

sein. Da aber, wenn $k < q - 1$ ist,

$$1.2.3\ldots\ldots k \equiv (-1)^k.(q-1)(q-2)\ldots(q-k)$$

$$\prod(q-1-k).\prod(k) \equiv (-1)^k.1.2.3\ldots(q-1) \equiv (-1)^{k+1} \pmod{q}$$

gefunden wird, so kann man auch schreiben:

$$\psi(q-1-\mu_{i-1}, q-1-m_i, \gamma) \equiv \frac{\Pi(\mu_{i-1}).\Pi(m_i)}{\Pi(\mu_{i-1}+m_i-q+1)} \pmod{q}$$

oder auch, da in diesem Falle $\mu_{i-1} + m_i = q - 1 + \mu_i$ ist,

$$(8) \qquad \frac{1}{\psi(q-1-\mu_{i-1}, q-1-m_i, \gamma)} \equiv \frac{\Pi(\mu_i)}{\Pi(\mu_{i-1}).\Pi(m_i)} \pmod{q}$$

wie in dem vorigen Falle.

Ist endlich drittens $\mu_{i-1} + m_i < q - 1$, so folgt nach demselben Satze

$$\psi(\mu_{i-1}, m_i, \gamma) \equiv -\frac{\Pi(\mu_{i-1}+m_i)}{\Pi(\mu_{i-1}).\Pi(m_i)} \pmod{q}$$

oder, da jetzt $\mu_{i-1} + m_i = \mu_i$ ist,

$$(9) \qquad \psi(\mu_{i-1}, m_i, \gamma) \equiv -\frac{\Pi(\mu_i)}{\Pi(\mu_{i-1}) \cdot \Pi(m_i)} \pmod{q} .$$

Setzt man daher in die Functionen $f(\omega)$ und $\varphi(\omega)$ statt ω die primitive Wurzel γ, und nimmt auf die im Vorigen angegebene Bildungsweise derselben aus den ψ-Functionen, den drei unterschiedenen Fällen entsprechend, Rücksicht, so wird man mit Beachtung der Congruenzen (7), (8) und (9) offenbar die folgende Congruenz finden:

$$(10) \qquad \frac{f(\gamma)}{\varphi(\gamma)} \equiv (-1)^{\alpha-1-n_\alpha} \cdot \frac{\Pi(\mu_\alpha)}{\Pi(m_1)\,\Pi(m_2) \ldots \Pi(m_\alpha)} \pmod{q} ,$$

da der dritte Fall $\alpha - 1 - n_\alpha$ Mal eintreten wird.

4. Wir werden jetzt speciell von folgendem Producte handeln:

$$\prod_a (\omega^{-a\mu}, R),$$

in welchem a jeden der $\frac{p-1}{2}$ quadratischen Reste von p bezeichnen soll, welche kleiner als p sind, und die Multiplication sich über alle diese Zahlen zu erstrecken hat. Um den Werth dieses Products zu erhalten, muss man in der Gleichung (4) $\alpha = \frac{p-1}{2}$ und die Zahlen $m_1, m_2, \ldots m_\alpha$ den verschiedenen Zahlen $a\mu$ gleich wählen. Wenn man nun aber in dem Ausdrucke

$$\psi(h,k) = \frac{(\omega^{-h}, R) \cdot (\omega^{-k}, R)}{(\omega^{-h-k}, R)}$$

für h, k Vielfache von μ, etwa $h = h'\mu$, $k = k'\mu$ setzt, und bezeichnet $\omega^{-\mu}$ mit r, sodass r eine primitive Wurzel der Gleichung $x^p = 1$ wird, so enthält der Ausdruck

$$\psi(h'\mu, k'\mu) = \frac{(r^{h'}, R) \cdot (r^{k'}, R)}{(r^{h'+k'}, R)}$$

nur noch die Wurzel r. Demnach wird auch in den beiden Functionen $f(\omega)$, $\varphi(\omega)$, welche sich in dem hier betrachteten Falle aus solchen ψ-Functionen zusammensetzen, nur r vorkommen können, deshalb sollen sie mit $f_a(r)$ und $\varphi_a(r)$, desgleichen $\Psi(\omega)$ durch $\Psi_a(r)$ bezeichnet werden. Wenn man ferner $\gamma^{-\mu} = u$ setzt, so werden die Functionen $f(\gamma)$, $\varphi(\gamma)$ in der Congruenz (10) durch $f_a(u)$, $\varphi_a(u)$ resp. zu ersetzen sein. Endlich wollen wir

bemerken, dass, wenn g irgend eine primitive Wurzel (mod. p) bedeutet, sämmtliche quadratische Reste von p den Potenzen $1, g^2, g^4, \ldots . g^{p-3}$ (mod. p) congruent sind, folglich wird die, auf alle oben definirten Zahlen a bezogene Summe

$$\sum_a a \equiv 1 + g^2 + g^4 + \ldots . + g^{p-3} \text{ (mod. } p)$$

d. h. congruent Null sein; Σa ist also eine durch p theilbare, desgleichen also auch $\underset{a}{\Sigma} a \mu$ eine durch $p\mu = q - 1$ theilbare ganze Zahl. Hiernach wird $\mu_a = 0$, $n_a = \frac{\underset{a}{\Sigma} a\mu}{q-1} = \frac{\Sigma a}{p}$ sein, und die Formeln (6) und (10) gehen in die folgenden über:

$$\Psi_a(r) = q^{\frac{\Sigma a}{p}} \cdot \frac{f_a(r)}{\varphi_a(r)} \tag{11}$$

$$\frac{f_a(u)}{\varphi_a(u)} \equiv -(-1)^{\frac{p-1}{2} - \frac{\Sigma a}{p}} \frac{1}{\underset{a}{\Pi}(1 \, . \, 2 \, . \, 3 \ldots . \mu a)} \text{ (mod. } q); \tag{12}$$

in dem Producte der letzten Formel muss wieder über alle oben definirten Zahlen a multiplicirt werden.

Bezeichnen wir ebenso mit b alle quadratischen Nichtreste von p, welche kleiner sind als p, und bilden das Product

$$\prod_b (\omega^{-b\mu}, R)$$

auf alle diese Werthe b bezogen, so gelten ganz dieselben Betrachtungen. Da

$$\sum b \equiv g + g^3 + g^5 + \ldots . + g^{p-2} \text{ (mod. } p)$$

also durch p theilbar ist, so ergiebt sich wieder $\mu_a = 0, n_a = \frac{\Sigma b}{p}$; bezeichnet man ferner mit $\Psi_b(r)$, $f_b(r)$, $\varphi_b(r)$ die auf diesen Fall bezüglichen Werthe der Functionen $\Psi(\omega)$, $f(\omega)$, $\varphi(\omega)$, so ergeben sich aus den Formeln (6) und (10) die nachstehenden:

$$\Psi_b(r) = q^{\frac{\Sigma b}{p}} \cdot \frac{f_b(r)}{\varphi_b(r)} \tag{13}$$

$$\frac{f_b(u)}{\varphi_b(u)} \equiv -(-1)^{\frac{p-1}{2} - \frac{\Sigma b}{p}} \cdot \frac{1}{\underset{b}{\Pi}(1 \, . \, 2 \, . \, 3 \ldots . \mu b)} \text{ (mod. } q). \tag{14}$$

5. Andererseits geht aus der Gleichung (4), wenn man

$\alpha = \frac{p-1}{2}$ und die Zahlen $m_1, m_2, \ldots . m_\alpha$ den Zahlen $a\mu$ gleich setzt, deren Summe als eine durch $q-1$ theilbare Zahl soeben nachgewiesen worden ist, folgende Gleichung

$$(15) \qquad \Psi_a(r) = -\prod_a (\omega^{-a\mu}, R) = -\prod_a (r^a, R)$$

hervor, da

$$(\omega^{-(m_1+m_2+\ldots+m_\alpha)}, R) = (\omega^{-\Sigma a\mu}, R) = -1$$

wird. Diese Gleichung lehrt aber, dass das Product eine, von R ganz unabhängige, nur aus r gebildete, ganze Function ist, deren Coëfficienten ganze Zahlen sein müssen, da die Coëfficienten in den einzelnen Factoren (r^a, R) solche Zahlen sind; es ist, mit andern Worten, eine, aus r zusammengesetzte, complexe ganze Zahl. Indessen ist dasselbe offenbar unveränderlich, wenn r durch irgend eine Potenz $r^{a'}$ ersetzt wird, worin a' selbst ein quadratischer Rest (mod. p) ist; denn die $\frac{p-1}{2}$ Zahlen aa' sind, wie leicht zu sehen, unter einander (mod. p) incongruent und wieder quadratische Reste, folglich stimmen ihre kleinsten positiven Reste, von der Ordnung abgesehen, auf welche es in dem Producte nicht ankommt, mit den Zahlen a im Ganzen überein. Da nun a' stets einer geraden Potenz von g, etwa g^{2h} (mod. p) congruent ist, und $r^{g^{2h}}$ derselben zweigliedrigen Periode angehört, wie r selber, kommt das Gesagte nach Nr. 5 der 6. Vorlesung darauf hinaus, dass das Product nicht eine Function der einzelnen Wurzeln der Gleichung $x^p = 1$, sondern vielmehr eine Function ihrer beiden zweigliedrigen Perioden, welche η_0, η_1 genannt werden mögen, sein muss. Man kann daher setzen:

$$(16) \qquad \prod_a (\omega^{-a\mu}, R) = A_0\eta_0 + A_1\eta_1,$$

worin A_0, A_1 ganze Zahlen bedeuten.

Genau ebenso findet sich, wie auch einfach durch Vertauschung von $\omega^{-\mu} = r$ mit einer der Wurzeln $r^{g^{2h+1}}$ d. h., da g^{2h+1} irgend einem Nichtreste (mod. p) congruent ist, mit einer der Wurzeln r^b hervorgeht,

$$(17) \qquad \prod_b (\omega^{-b\mu}, R) = A_0\eta_1 + A_1\eta_0,$$

auch ist

$$\Psi_b(r) = -\prod_b (\omega^{-b\mu}, R)\,. \tag{18}$$

Wenn wir uns von nun an auf die Voraussetzung, dass p die Form $4n + 3$ habe, beschränken, so können wir die Gleichung (17) etwas anders schreiben; denn vermittelst der Bemerkung, dass dann -1 ein quadratischer Nichtrest von p ist, und dass folglich die Zahlen $-b$ allen quadratischen Resten (mod. p) congruent sind, nimmt sie offenbar folgende Gestalt an:

$$\prod_a (\omega^{a\mu}, R) = A_0\eta_1 + A_1\eta_0\,.$$

Erinnern wir uns hier, dass nach Formel (29) der 8. Vorl.

$$(\omega^{a\mu}, R)\,.\,(\omega^{-a\mu}, R) = (-1)^{a\mu}\,.\,q$$

ist, dann werden wir durch Verbindung der vorigen Gleichung mit der Gleichung (16), wenn wir beachten, dass die Anzahl der Factoren in jedem der beiden Producte gleich $\frac{p-1}{2}$, sowie dass $\sum_a a\mu$ durch $q-1$ theilbar, also eine gerade Zahl ist, zu der folgenden Gleichung:

$$q^{\frac{p-1}{2}} = (A_0\eta_0 + A_1\eta_1)\,(A_0\eta_1 + A_1\eta_0)$$

gelangen, welche, wenn für die Perioden ihre in Nr. 2 der 15. Vorlesung gefundenen Werthe

$$\eta_0 = \frac{-1+\sqrt{-p}}{2}, \quad \eta_1 = \frac{-1-\sqrt{-p}}{2}$$

substituirt werden, in die andere Gestalt:

$$4\,.\,q^{\frac{p-1}{2}} = (A_0 + A_1)^2 + p(A_0 - A_1)^2 \tag{19}$$

übergeht.

6. Die so gewonnene Formel kann noch vereinfacht werden, wenn man sie durch die höchste Potenz von q, welche den Quadraten $(A_0 + A_1)^2$ und $(A_0 - A_1)^2$ gemeinsam sein kann, dividirt. Zur Bestimmung dieser Potenz dienen aber die Relationen (11) bis (14), von denen die erste und dritte, wenn angenommen wird, die höchste, den Zahlen A_0, A_1 gemeinsame, Potenz von q sei q^t,

mit Rücksicht auf (16) und (17) auch so geschrieben werden können:

$$(20)\quad \begin{cases} \dfrac{A_0}{q^t}\cdot\eta_0 + \dfrac{A_1}{q^t}\cdot\eta_1 = -q^{\frac{\Sigma a}{p}-t}\cdot\dfrac{f_a(r)}{\varphi_a(r)} \\ \dfrac{A_0}{q^t}\cdot\eta_1 + \dfrac{A_1}{q^t}\cdot\eta_0 = -q^{\frac{\Sigma b}{p}-t}\cdot\dfrac{f_b(r)}{\varphi_b(r)}. \end{cases}$$

Wir wollen nun zwischen den Wurzeln der Gleichung

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$$

und den Wurzeln der Congruenz

$$x^{p-1} + x^{p-2} + \ldots + x + 1 \equiv 0 \pmod{q}$$

genau dieselbe Correspondenz herstellen, wie in Nr. 2 der vor. Vorlesung, bei welcher u^h die zu r^h gehörige Congruenzwurzel war. Dann ist zunächst leicht nachzuweisen, dass keine der Zahlen $\frac{\Sigma a}{p}$, $\frac{\Sigma b}{p}$ kleiner als t sein kann; denn wäre z. B. $\frac{\Sigma a}{p} < t$, so entstünde aus der ersten der vorhergehenden Gleichungen die folgende:

$$q^{t-\frac{\Sigma a}{p}}\cdot\left(\frac{A_0}{q^t}\cdot\eta_0 + \frac{A_1}{q^t}\cdot\eta_1\right) = -\frac{f_a(r)}{\varphi_a(r)},$$

und diese ginge nach dem Hauptsatze in Nr. 6 der 17. Vorlesung durch Substitution der Congruenzwurzeln statt der zugehörigen Gleichungswurzeln in die richtige Congruenz:

$$q^{t-\frac{\Sigma a}{p}}\cdot\left(\frac{A_0}{q^t}\cdot u_0 + \frac{A_1}{q^t}\cdot u_1\right) \equiv -\frac{f_a(u)}{\varphi_a(u)} \pmod{q},$$

in welcher

$$u_0 = u + u^{g^2} + \ldots + u^{g^{p-3}}$$

$$u_1 = u^g + u^{g^3} + \ldots + u^{g^{p-2}}$$

gesetzt ist, über und lieferte $\frac{f_a(u)}{\varphi_a(u)} \equiv 0 \pmod{q}$, was mit der Congruenz (12) unverträglich ist.

Wenn hierdurch nachgewiesen ist, dass die Zahlen $\frac{\Sigma a}{p}$, $\frac{\Sigma b}{p}$ mindestens gleich t sein müssen, so zeigen die Congruenzen:

$$(21)\qquad \left.\begin{aligned} \frac{A_0}{q^t}\cdot u_0 + \frac{A_1}{q^t}\cdot u_1 &\equiv -q^{\frac{\Sigma a}{p}-t}\cdot\frac{f_a(u)}{\varphi_a(u)} \\ \frac{A_0}{q^t}\cdot u_1 + \frac{A_1}{q^t}\cdot u_0 &\equiv -q^{\frac{\Sigma b}{p}-t}\cdot\frac{f_b(u)}{\varphi_b(u)} \end{aligned}\right\}\ (\text{mod. } q),$$

welche aus den Gleichungen (20) entstehen, indem die Gleichungswurzeln durch die zugehörigen Congruenzwurzeln ersetzt werden, dass nicht beide Zahlen grösser als t sein können. Denn sonst würde

$$(22)\ \text{folglich}\quad \left.\begin{aligned} A_0u_0 + A_1u_1 \equiv 0,\ A_0u_1 + A_1u_0 \equiv 0 \\ A_0(u_0^2 - u_1^2) \equiv 0,\ A_1(u_0^2 - u_1^2) \equiv 0 \end{aligned}\right\}\ (\text{mod. } q^{t+1}).$$

Es ist aber $u_0^2 - u_1^2 = (u_0 + u_1)(u_0 - u_1)$; von diesen Factoren ist der erste der negativen Einheit (mod. q) congruent, da

$$u_0 + u_1 = u + u^g + u^{g^2} + \ldots . + u^{g^{p-2}} \equiv u + u^2 + \ldots . + u^{p-1}$$

und

$$1 + u + u^2 + \ldots . + u^{p-1} \equiv 0 \ (\text{mod. } q)$$

ist. Da ferner die Gleichung besteht

$$(\eta_0 - \eta_1)^2 = -p,$$

so erhält man die Congruenz

$$(u_0 - u_1)^2 \equiv -p \ (\text{mod. } q),$$

welche lehrt, dass auch der andere Factor, und folglich auch $u_0^2 - u_1^2$ nicht durch q theilbar ist. Demnach ergäbe sich aus den Congruenzen (22) das, der Bedeutung des Exponenten t widerstreitende Resultat, dass A_0 und A_1 durch q^{t+1} theilbar wären.

Aus diesen Betrachtungen ergiebt sich, dass, wenn nicht etwa $\frac{\Sigma a}{p}$, $\frac{\Sigma b}{p}$ gleichen Werth haben, t jedenfalls dem kleinern derselben gleich sein muss. Aber jene Voraussetzung ist unzulässig, da $\Sigma a + \Sigma b$ gleich der Summe

$$1 + 2 + 3 + \ldots . + (p-1) = \frac{p(p-1)}{2}$$

in dem hier betrachteten Falle also, in welchem $\frac{p-1}{2}$ ungerade ist, einer ungeraden Zahl gleich ist, weshalb $\Sigma b - \Sigma a$ nicht gerade also auch nicht Null sein kann. Dasselbe folgt allgemein aus einem andern, bald zu erwähnenden Umstande, aus

welchem wir auch schliessen werden, dass Σb der grössere der beiden Werthe ist. Folglich muss $t = \frac{\Sigma a}{p}$ sein.

Wenn man nunmehr die Gleichung (19) mit dem Quadrate der grössten, den Zahlen A_0, A_1 oder den Zahlen $A_0 + A_1$, $A_0 - A_1$ gemeinsamen Potenz von q dividirt und

$$(23) \qquad \frac{A_0 + A_1}{q^t} = x, \quad \frac{A_0 - A_1}{q^t} = y$$

setzt, sowie bemerkt, dass $\frac{\Sigma a}{p} + \frac{\Sigma b}{p} = \frac{p-1}{2}$ ist, so ergiebt sich endlich folgende höchst beachtenswerthe Gleichung:

$$(24) \qquad 4 \,.\, q^{\frac{\Sigma b - \Sigma a}{p}} = x^2 + py^2,$$

welche den Satz enthält:

Ist p eine Primzahl von der Form $4n + 3$, q eine Primzahl von der Form $\mu p + 1$, und bezeichnen Σa, Σb die Summe resp. aller quadratischen Reste und Nichtreste (mod. p), welche kleiner als p sind, so gestattet das Vierfache der Potenz $q^{\frac{\Sigma b - \Sigma a}{p}}$ eine Darstellung durch die Form $x^2 + py^2$.

Die Congruenzen (21) können jetzt folgendermassen geschrieben werden, wenn auf (12) Rücksicht genommen wird:

$$\left.\begin{aligned} \frac{A_0}{q^t} \,.\, u_0 + \frac{A_1}{q^t} \,.\, u_1 &\equiv (-1)^{\frac{\Sigma b}{p}} \,.\, \frac{1}{\underset{a}{\Pi}(1 \,.\, 2 \,.\, 3 \ldots a\mu)} \\ \frac{A_0}{q^t} \,.\, u_1 + \frac{A_1}{q^t} \,.\, u_0 &\equiv 0 \end{aligned}\right\} \pmod{q}$$

und geben durch Addition die, zur Bestimmung von x dienende Congruenz

$$(25) \qquad x \equiv -(-1)^{\frac{\Sigma b}{p}} \,.\, \frac{1}{\underset{a}{\Pi}(1 \,.\, 2 \,.\, 3 \ldots \mu a)} \pmod{q}.$$

So erhält man den Zusatz: Die Zahl x in der Darstellung (24) leistet der Congruenz (25) Genüge.

Noch kann beachtet werden, dass in dem Falle, wo p die Form $8n + 7$ hat, die Darstellung durch gerade Zahlen x, y geschieht; denn, wären sie, was sonst nothwendig wäre, da $x^2 + py^2$ gerade werden soll, Beide ungerade, so würden x^2, y^2 durch 8 getheilt den Rest 1 geben, $x^2 + py^2$ also durch 8 theil-

bar sein, während die andere Seite der Gleichung (24) es nur durch 4 ist. Setzt man daher $x = 2\xi$, $y = 2\eta$, so ergiebt sich der Folgesatz:

Ist p eine Primzahl von der Form $8n + 7$ und q eine Primzahl von der Form $\mu p + 1$, so giebt es ganze Zahlen ξ, η von der Beschaffenheit, dass

$$q^{\frac{\Sigma b - \Sigma a}{p}} = \xi^2 + p \cdot \eta^2$$

ist, während ξ der Congruenz

$$2\xi \equiv -(-1)^{\frac{\Sigma b}{p}} \frac{1}{\Pi_a (1 \cdot 2 \cdot 3 \ldots \mu a)} \pmod{q}$$

Genüge leistet.

Ist z. B. $q = 7\mu + 1$, so findet sich, da unter den Zahlen, welche kleiner als 7 sind, die Zahlen 1, 2, 4 die quadratischen Reste, die übrigen Zahlen 3, 5, 6 die quadratischen Nichtreste von 7 sind,

$$(26) \begin{cases} q = \xi^2 + 7 \cdot \eta^2 \\ \text{wenn} \\ \xi \equiv -\frac{1}{2} \cdot \frac{1}{\Pi\mu \cdot \Pi 2\mu \cdot \Pi 4\mu} \pmod{q} \\ \text{ist, wofür man auch} \\ \xi \equiv \frac{1}{2} \cdot \frac{\Pi 3\mu}{\Pi\mu \cdot \Pi 2\mu} \pmod{q} \end{cases}$$

setzen kann, wenn man bemerkt, dass nach Wilson's Satze

$$-1 \equiv \prod 7\mu \equiv \prod 4\mu \cdot (4\mu + 1)(4\mu + 2) \ldots 7\mu$$
$$\equiv (-1)^{3\mu} \cdot 1 \cdot 2 \cdot 3 \ldots 3\mu \cdot \prod 4\mu \pmod{q}$$

ist, und μ nothwendig eine gerade Zahl sein muss. Dieses Resultat findet sich bereits in der in Nr. 3 der 11. Vorlesung citirten kleinen Abhandlung von Jacobi. —

Es ist zu beachten, dass die Zahlen ξ, η durch die Bedingungen (26) vollständig bestimmt sind, nämlich ξ als absolut kleinster Rest von q, welcher der Congruenz genügt, sodann η durch die quadratische Formel. Wenn jedoch in der Gleichung (24) eine höhere als die erste Potenz von q zur Linken des Gleichheitszeichens steht, wird die Darstellung durch die Bedingungen (24) und (25) im Allgemeinen noch nicht vollständig bestimmt sein. Während wir einige darauf bezügliche Einzelheiten hier übergehen wollen,

müssen wir noch auf den Zusammenhang, welcher zwischen diesen Betrachtungen und einer wichtigen Frage aus der Theorie der quadratischen Formen besteht, soweit es ohne näheres Eingehen auf diese Theorie möglich ist, hinweisen.

7. Man versteht in der Zahlentheorie unter einer (binären) quadratischen Form jeden Ausdruck von der folgenden Gestalt:

$$ax^2 + 2bxy + cy^2,$$

in welchem die Coëfficienten a, b, c ganze Zahlen sind; der Ausdruck $b^2 - ac$ heisst die Determinante der Form. Zwei solche Formen

$$ax^2 + 2bxy + cy^2,\quad a'x'^2 + 2b'x'y' + c'y'^2$$

von gleicher Determinante werden äquivalent oder zu derselben Classe gehörig genannt, wenn die erste in die zweite mittelst einer linearen Transformation

$$x = \alpha x' + \beta y',\quad y = \gamma x' + \delta y'$$

übergeführt werden kann, in welcher die Coëfficienten α, β, γ, δ ganze, der Gleichung $\alpha\delta - \beta\gamma = 1$ genügende Zahlen sind. Haben die Coëfficienten a, $2b$, c der Form keinen gemeinschaftlichen Theiler, so heisst sie eigentlich primitiv, wenn sie den grössten gemeinsamen Theiler Zwei haben, uneigentlich primitiv.

Denkt man sich nun alle uneigentlich primitiven Formen der Determinante $-p$, so zerfallen diese in eine gewisse, stets endliche Anzahl H verschiedener Classen von, unter einander äquivalenten, Formen. Die Bemerkung aber, welche wir hier anschliessen wollten, besteht darin, dass, wie Dirichlet auf höchst merkwürdige Weise, indem er die Analysis mit der Zahlentheorie in Verbindung brachte, nachgewiesen hat, die Zahl H genau gleich dem Exponenten von q in der Gleichung (24) nämlich

$$H = \frac{\Sigma b - \Sigma a}{p}$$

ist. Es ist hier nicht der Ort, auf Dirichlet's Methoden näher einzugehen, vielmehr muss auf seine betreffenden Arbeiten, deren wesentlichste in den Bänden 19, 21, 24 des Crelle'schen Journals enthalten sind, oder auch auf seine Vorlesungen über Zahlentheorie verwiesen werden. Nur das Eine muss zur Ergänzung des oben Gesagten hinzugefügt werden, dass aus dem Dirichlet-

schen Resultate unmittelbar die Beziehung $\Sigma b > \Sigma a$ hervorgeht, da die Anzahl H der Classen ihrer Natur nach stets eine positive ganze Zahl sein muss. Auf anderm Wege ist derselbe Umstand bisher nicht bewiesen worden, auch dürfte es, um mit Dirichlet zu reden*), nicht leicht sein, dafür einen arithmetischen Beweis zu finden.

Zum Schluss ist auf eine Notiz von Jacobi**) hinzuweisen, welche besonders geeignet ist, den Scharfsinn dieses grossen Mathematikers zu bezeugen. Die Theorie der quadratischen Formen lehrt, dass, wenn das Doppelte einer Primzahl q überhaupt durch uneigentlich primitive Formen der Determinante $-p$ darstellbar ist, es stets eine gewisse kleinste ganze Zahl h giebt von der Beschaffenheit, dass $2 \cdot q^h$ durch die sogenannte Hauptform

$$2x^2 + 2xy + \frac{p+1}{2} y^2$$

darstellbar ist; diese Zahl h muss stets gleich der Classenzahl H oder wenigstens ein Divisor derselben, und jede grössere Zahl derselben Beschaffenheit muss ein Vielfaches von der kleinsten Zahl h sein. Bemerken wir nun, dass die Zahlen x, y in der Gleichung (24) entweder Beide gerade, oder Beide ungerade sein müssen, damit die Summe $x^2 + py^2$ eine gerade Zahl wird, so ist klar, dass, wenn

$$x = 2X + Y, \; y = Y$$

gesetzt wird, für X, Y ganzzahlige Werthe sich ergeben werden. Durch diese Transformation geht aber die Form $x^2 + py^2$ in

$$2\left(2X^2 + 2XY + \frac{p+1}{2} Y^2\right)$$

über, und aus der Gleichung (24) ergiebt sich die folgende:

$$2 \cdot q^{\frac{\Sigma b - \Sigma a}{p}} = 2X^2 + 2XY + \frac{p+1}{2} Y^2.$$

Hieraus folgt nach dem eben Bemerkten jedenfalls, dass die Anzahl H der Classen uneigentlich primitiver Formen von der Determinante $-p$ mit der Zahl $\frac{\Sigma b - \Sigma a}{p}$ in einem einfachen Verhältnisse stehen wird. Da Jacobi aber bei einer Reihe von

*) s. Abhandl. d. Berl. Academie Jahrg. 1837 pag. 57.

**) in Crelle's J. Bd. 9 pag. 189.

Beispielen fand, dass H dieser Zahl selbst gleich wurde, sprach er den Satz aus, dass überhaupt die Classenanzahl H durch die Formel

$$H = \frac{\Sigma b - \Sigma a}{p}$$

bestimmt werde, ein Satz, der, wie schon gesagt wurde, durch Dirichlet's Forschungen eine glänzende Bestätigung gefunden hat.

8. Doch wir wenden uns nunmehr zu der letzten Anwendung, welche wir von der Kreistheilung machen wollen; sie betrifft einen, für die Theorie der quadratischen Formen von positiver Determinante wichtigen Gegenstand. Wenn wir uns auch hier auf den einfachsten Fall beschränken, in welchem die Determinante eine positive Primzahl p ist, so spielt in der Theorie der Formen von solcher Determinante die Aufgabe, alle ganzzahligen Lösungen t, u der sogenannten Pell'schen Gleichung

$$t^2 - pu^2 = 1$$

zu finden, eine grosse Rolle. Da man indessen aus einer Auflösung, bei welcher u von Null verschieden ist, leicht alle übrigen finden kann, kommt es wesentlich darauf an, eine solche zu finden, und es ist nun sehr merkwürdig, dass auch hierzu die Kreistheilung das Mittel darbietet und gerade diejenige Auflösung finden lehrt, welche wieder zur Anzahl der Classen äquivalenter Formen von der Determinante p eine unmittelbare Beziehung hat.

Um dahin zu gelangen, müssen wir von den Resultaten der Nr. 3 der 15. Vorlesung unsern Ausgang nehmen. Wir haben dort die Formel erhalten:

$$(27) \qquad 4 \cdot \frac{x^p - 1}{x - 1} = Y(x)^2 - (-1)^{\frac{p-1}{2}} \cdot pZ(x)^2 \,.$$

Unterscheiden wir nun von vornherein die beiden Fälle, in denen p die Form $4n + 1$ oder die Form $4n + 3$ hat.

In dem erstern erhalten wir aus (27) durch die Substitution $x = 1$ folgende Formel:

$$(28) \qquad 4p = y^2 - pz^2$$

wenn mit y, z die reellen ganzen Zahlen bezeichnet werden, in welche die Functionen $Y(x)$, $Z(x)$ bei solcher Substitution übergehen, und welche Beide von Null verschieden sind, da weder $4p = y^2$, noch $4p = -pz^2$ sein kann. Die Gleichung (28) lehrt

ausserdem, dass y durch p theilbar ist; setzt man also $y=p.y_0$ und der Uebereinstimmung wegen $z=z_0$, so ergiebt sich nach Division mit p

(29) $$z_0^2 - py_0^2 = -4 .$$

Diese Gleichung kann man auch so schreiben:

$$(z_0 + y_0 \sqrt{p})(z_0 - y_0 \sqrt{p}) = -4,$$

und durch ihre Quadrirung findet man, wenn man

$$(z_0 + y_0 \sqrt{p})^2 = (z_0^2 + py_0^2) + 2z_0 y_0 \sqrt{p} = z_1 + y_1 \sqrt{p}$$

setzt,

(30) $$(z_1 + y_1 \sqrt{p})(z_1 - y_1 \sqrt{p}) = 16 .$$

Die ganzen Zahlen

$$z_1 = z_0^2 + py_0^2, \; y_1 = 2z_0 y_0$$

sind jedenfalls durch Zwei theilbar, wie für y_1 von selbst klar ist und für z_1 sich daraus ergiebt, dass man wegen (29) auch

$$z_1 = -4 + 2py_0^2$$

schreiben kann. Sind aber y_0, z_0 schon gerade Zahlen, so werden z_1, y_1 sogar durch Vier theilbar sein, und man findet dann

$$\left(\frac{z_1}{4} + \frac{y_1}{4}\sqrt{p}\right)\left(\frac{z_1}{4} - \frac{y_1}{4}\sqrt{p}\right) = 1$$

d. h. $t = \frac{z_1}{4}$, $u = \frac{y_1}{4}$ ist eine ganzzahlige Auflösung der Pell'schen Gleichung

$$t^2 - pu^2 = 1$$

von der gesuchten Art, da y_0, z_0, y_1, u von Null verschieden sind. Dieser Fall tritt stets ein, wenn p die Form $8n+1$ hat.

Wenn dagegen z_0, y_0 ungerade sind, was sie, damit $z_0^2 - py_0^2$ gerade werde, gleichzeitig sein müssen, wenn sie nicht Beide gerade sind, so sind y_1, z_1 nur durch 2 theilbar, also z_2, y_2 ungerade, wenn man

$$z_1 = 2z_2, \; y_1 = 2y_2$$

setzt, und es ergiebt sich dann aus (30)

$$(z_2 + y_2 \sqrt{p})(z_2 - y_2 \sqrt{p}) = 4 .$$

Erhebt man diese Gleichung zum Cubus und setzt

$$(z_2 + y_2\sqrt{p})^3 = (z_2^3 + 3pz_2 y_2^2) + (3z_2^2 y_2 + py_2^3).\sqrt{p} = z_3 + y_3\sqrt{p},$$

so übersieht man leicht, dass z_3, y_3 Beide durch 8 theilbar sind;

denn, da jetzt p die Form $8n+5$ haben muss, so ergiebt sich

$$z_2^2 + 3py_2^2 \equiv 0,\ 3z_2^2 + py_2^2 \equiv 0 \pmod{8}.$$

Da nun

$$(z_3 + y_3\sqrt{p})(z_3 - y_3\sqrt{p}) = 64$$

ist, findet man

$$\left(\frac{z_3}{8} + \frac{y_3}{8}\sqrt{p}\right)\left(\frac{z_3}{8} - \frac{y_3}{8}\sqrt{p}\right) = 1;$$

also sind die beiden ganzen Zahlen $t = \frac{z_3}{8}$, $u = \frac{y_3}{8}$ eine Lösung der Pell'schen Gleichung

$$t^2 - pu^2 = 1.$$

9. In dem zweiten Falle, wo p die Form $4n+3$ hat, würde die Substitution $x=1$ in der Gleichung (27) nur zu einer Identität führen. Wenn man dagegen $x=i$ setzt, so wird sich ein ähnliches Resultat ergeben, wie im vorigen Falle. Nach den Formeln (18) in Nr. 3 der 15. Vorlesung folgt bei dieser Substitution

$$Y(i) = -i^{\frac{p-1}{2}}.\,Y(-i),\ Z(i) = i^{\frac{p-1}{2}}.\,Z(-i).$$

Die Functionen $Y(i)$ und $Z(i)$ sind aber ganze complexe Zahlen von den Formen $y' + y''i$ und $z' + z''i$ resp. Wenn daher zunächst p die Form $8n+3$ hat, so geben die vorigen Gleichungen folgende Beziehungen:

$$y' + y''i = -i(y' - y''i),\ z' + z''i = i(z' - z''i)$$

d. h.

$$y' = -y'',\ z' = z'',$$

folglich werden $Y(i)$, $Z(i)$ von den Formen:

$$Y(i) = y'(1-i),\ Z(i) = z'(1+i).$$

Ist dagegen p von der Form $8n+7$, so erhält man die Beziehungen:

$$y' + y''i = i(y' - y''i),\ z' + z''i = -i(z' - z''i),$$

aus denen $y' = y''$, $z' = -z''$ also

$$Y(i) = y'(1+i),\ Z(i) = z'(1-i)$$

hervorgeht.

Da andererseits $\frac{x^p-1}{x-1}$ für $x=i$ in $\frac{i^p-1}{i-1}$ übergeht, erhält es, wenn p die Form $4n+3$ hat, den Werth i, und die

Gleichung (27) ergiebt demnach die nachstehende:

$$4i = y'^2 (1 \pm i)^2 + pz'^2 (1 \mp i)^2,$$

in welcher die doppelten Zeichen mit einander correspondiren, oder einfacher, da $(1 \pm i)^2 = \pm 2i$ ist,

$$(31) \qquad y'^2 - pz'^2 = \pm 2,$$

was wir auch so schreiben können:

$$(y' + z'\sqrt{p})(y' - z'\sqrt{p}) = \pm 2\,.$$

Erhebt man nun die letzte Gleichung in's Quadrat und setzt

$$(y' + z'\sqrt{p})^2 = y'^2 + pz'^2 + 2y'z'\sqrt{p} = y'_1 + z'_1\sqrt{p},$$

so sind

$$y_1' = y'^2 + pz'^2 = \pm 2 + 2pz'^2, \quad z_1' = 2y'z'$$

gerade Zahlen, welche der Gleichung

$$(y_1' + z'_1\sqrt{p})(y_1' - z_1'\sqrt{p}) = 4$$

Genüge leisten, und $t = \frac{y_1'}{2}$, $u = \frac{z_1'}{2}$ zwei ganze Zahlen, für welche

$$(t + u\sqrt{p})(t - u\sqrt{p}) = 1$$

ist, d. h. eine ganzzahlige Lösung der Pell'schen Gleichung.

10. Hierdurch ist nachgewiesen, dass sich aus der Kreistheilung stets eine ganzzahlige Auflösung der Pell'schen Gleichung ableiten lässt. Diese ist jedoch nicht diejenige Auflösung, welche man als ihre Fundamentalauflösung zu bezeichnen pflegt, bei welcher nämlich die Zahlen t, u die kleinsten positiven Zahlen sind. Fragt man nun, in welcher Beziehung die so gefundenen Auflösungen zu der Fundamentalauflösung T, U stehen, so giebt die Antwort merkwürdiger Weise wieder einen innigen Zusammenhang zwischen der Kreistheilung und der Theorie der quadratischen Formen, insbesondere mit der Bestimmung der Classenanzahl zu erkennen. In der That, wenn wir uns der Kürze wegen auf den Fall einer positiven Determinante p von der Form $4n + 1$ beschränken, so folgt aus den von Dirichlet gefundenen Ausdrücken für die Anzahl H der Classen äquivalenter Formen von einer solchen Determinante folgende interessante Beziehung:

$$(32) \qquad (T + U\sqrt{p})^H = \left(\frac{y + z\sqrt{p}}{y - z\sqrt{p}}\right)^{2 - \left(\frac{2}{p}\right)},$$

wenn y, z die in Gleichung (28) vorkommenden ganzen Zahlen nämlich die Werthe $Y(1)$ und $Z(1)$ bedeuten, *eine Beziehung, welche den Zusammenhang der, aus der Kreistheilung gewonnenen Auflösung mit der Fundamentalauflösung der Pell'schen Gleichung bezeichnet.*

Dies Resultat giebt endlich noch zu einer Bemerkung Anlass, welche der über das Zeichen $\Sigma b - \Sigma a$ in Nr. 7 gemachten analog ist; *die ganzen Zahlen* y, z *sind nämlich positiv.* In der That, nach den Formeln in Nr. 3 der 15. Vorlesung ist

$$y + z\sqrt{p} = 2A(1) = 2\prod_a (1 - r^a), \; y - z\sqrt{p} = 2B(1) = 2\prod_b (1 - r^b).$$

Ist nun a ein quadratischer Rest, welcher grösser als $\frac{p}{2}$ ist, so wird, da -1 hier zu den quadratischen Resten gehört, $p - a$ ein quadratischer Rest sein, welcher $< \frac{p}{2}$ ist, und umgekehrt. Daraus folgt leicht, dass man, wenn a jetzt alle quadratischen Reste bezeichnet, welche $< \frac{p}{2}$ sind, setzen kann:

$$y + z\sqrt{p} = 2 \cdot \prod_a (1 - r^a)(1 - r^{-a})$$

oder, da $(1 - r^a)(1 - r^{-a}) = 2\left(1 - \cos\frac{2a\pi}{p}\right) = 4\sin^2\frac{2a\pi}{p}$, und die Anzahl der Werthe a gleich $\frac{p-1}{4}$ ist,

$$y + z\sqrt{p} = 2^{\frac{p+1}{2}} \cdot \left(\prod_a \sin\frac{2a\pi}{p}\right)^2.$$

Ganz ebenso findet man

$$y - z\sqrt{p} = 2^{\frac{p+1}{2}} \cdot \left(\prod_b \sin\frac{2b\pi}{p}\right)^2,$$

wenn man in dem Producte über alle quadratischen Nichtreste multiplicirt, die $< \frac{p}{2}$ sind. Diese Gleichungen lehren durch ihre Addition, dass y wesentlich positiv sein muss. Da aber T und U positiv sind, und

$$(T + U\sqrt{p})(T - U\sqrt{p}) = 1$$

ist, muss $T + U\sqrt{p} > 1$, folglich nach Gleichung (32)

$$\frac{y + z\sqrt{p}}{- z\sqrt{p}} > 1$$

sein, was nur geschehen kann, wenn auch z positiv ist. Auch diese Bemerkung ist bisher direct noch nicht bewiesen worden. —

Schliesslich mag erwähnt werden, dass, wenn man von den Darstellungen von $27X$ und $256X$ durch eine cubische resp. biquadratische Form ausgeht, welche durch die Gleichungen (40) der 15. und (39) der 16. Vorlesung gegeben werden, ähnliche Resultate, wie die hier aus der Darstellung von $4X$ durch eine quadratische Form abgeleiteten, gefunden werden können, wie es in Bezug auf die cubische Form in einer grossen Abhandlung von Eisenstein nachzulesen ist.*) Da es die Grenzen dieser Vorlesungen nicht gestatten, hierüber, noch auch über die wichtigen Forschungen Dirichlet's, die Classenanzahl betreffend, Ausführlicheres hier beizufügen, müssen wir den Leser, welcher darüber weiter unterrichtet zu sein wünscht, auf die bezüglichen Abhandlungen verweisen. —

*) Eisenstein, allgemeine Untersuchungen über die Formen 3ten Grades mit drei Variabeln, welche der Kreistheilung ihre Entstehung verdanken, in Cr. J. Bd. 28.

Druckfehlerverzeichniss.

Auf Seite 8 Zeile 2 v. o. lies: **statt**;
" " 32 Zeile 14 v. u. lies $f(x)$ statt (x).
" " 61 soll in der Fig. 1 der Punkt O nicht mit H, sondern mit G verbunden sein.
" " 64 letzte Zeile lies oder statt der.
" " 67 in der Figur lies J statt Y.
" " 68 Zeile 9 v. u. lies $2^{m'(2n+1)}$ statt $2^{m(2n+1)}$.
" " 82 Zeile 1 v. o. lies die ef-gliedrigen statt die ef-gliedrigen.
" " 105 Zeile 17 v. o. lies (12^a) statt (12^b).
" " 128 Zeile 4 v. u. lies ind. μ statt ind. μ'.
" " 134 Zeile 20 v. o. liess: statt.
" " 143 Zeile 3 v. u. lies $\frac{p-1}{2}$ statt $p-1$.
" " 209 Zeile 4 v. o. lies $\underset{\alpha}{\Sigma} r^{2\alpha}$ statt $\Sigma r^{2\alpha}$.
" " 215 Zeile 4 v. o. lies $\equiv$ statt $=$.
" " 218 Zeile 16 v. o. lies $+$ statt $-$.
" " 228 Zeile 7 v. u. lies $\eta_0\eta_1\eta_2 + \eta_0\eta_1\eta_3$ statt $\eta_0\eta_1\eta_3 + .\eta_0\eta_1\eta_3$.
" " 240 Zeile 3 v. o. lies (mod. q) statt (mod. p).

c

e_1 f_3









